Docket No.: 62807-037 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#6

In re Application of	:	
Shinji ITOH, et al.	:	
Serial No.: 10/074,239	:	Group Art Unit: 2131
Filed: February 14, 2002	:	Examiner:

For: NETWORK SYSTEM ENABLING TRANSMISSION CONTROL

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Honorable Commissioner for Patents and Trademarks
Washington, D. C. 20231

Sir:

At the time the above application was filed, priority was claimed based on the following application:

Japanese Patent Application No. 2001-370824, filed December 5, 2001

A copy of each priority application listed above is enclosed.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202)756-8000 KEG:prp
Facsimile: (202)756-8087
Date: July 16, 2002

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年１２月　５日

出願番号
Application Number: 特願２００１－３７０８２４

[ST.10/C]: [ＪＰ２００１－３７０８２４]

出願人
Applicant(s): 株式会社日立製作所

２００２年　２月２２日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００２－３００９４４２

【書類名】　特許願

【整理番号】　K01014091A

【あて先】　特許庁長官

【国際特許分類】　H04L 12/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　伊藤　信治

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　宮崎　邦彦

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　越前　　功

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　送信制御可能なネットワークシステム

【特許請求の範囲】

【請求項１】

組織内ネットワークに接続され、データを送受信する手段を備える送受信端末と、前記送受信端末と前記組織内ネットワークとの間で送受信されるデータを中継する手段を備える中継装置とを備えるネットワークシステムであって、

前記データは情報本体と前記情報本体に関連した付加情報からなり、

前記中継装置は前記付加情報を用いて送受信端末からのデータの送信を制御する手段と、前記組織内ネットワーク外へ送信可能な前記データから前記付加情報を取り除く手段を備える送信制御可能なネットワークシステム。

【請求項２】

請求項１記載の送信制御可能なネットワークシステムであって、

前記付加情報は前記情報本体の属性を表す情報を有し、

前記中継装置は前記属性に応じた送信ポリシーを保持する手段と、

前記送信ポリシーに従って前記送受信端末が送信したデータの送信の可否を決定する手段とを備える

送信制御可能なネットワークシステム。

【請求項３】

請求項１または請求項２記載の送信制御可能なネットワークシステムであって

、

前記属性は機密レベルである

送信制御可能なネットワークシステム。

【請求項４】

請求項３記載の送信制御可能なネットワークシステムであって、

さらに、前記付加情報は前記機密レベルの設定者情報と、前記設定者の階級情報を有する、送信制御可能なネットワークシステム。

【請求項５】

請求項３または請求項４に記載の送信制御可能なネットワークシステムであって、

前記送受信端末は前記付加情報を用いた前記情報本体へのアクセス制御手段と、

前記データの内、情報本体を、当該送受信端末で動作するアプリケーションプログラムに渡す手段とを備える、送信制御可能なネットワークシステム。

【請求項６】

請求項４記載の送信制御可能なネットワークシステムであって、

さらに、前記付加情報を変更する手段を備える、送信制御可能なネットワークシステム。

【請求項７】

請求項５または請求項６記載の送信制御可能なネットワークシステムであって、

前記アクセス制御手段は、前記アプリケーションプログラムに機密レベルを設定する手段と、前記アプリケーションプログラムのデータアクセス要求に対して、前記アプリケーションプログラムの機密レベルとデータ本体の機密レベルを比較することによって、前記アプリケーションプログラムの前記データへのアクセスの可否を決定する手段を備え、

前記アプリケーションプログラムに機密レベルを設定する手段は、の機密レベルは、当該アプリケーションプログラムが前記データの処理を開始する時に当該データ本体の機密レベルに応じて、前記アプリケーションプログラムに機密レベルを決定することを特徴とする、送信制御可能なネットワークシステム。

【請求項８】

請求項１記載の送信制御可能なネットワークシステムであって、前記中継装置は、

前記送受信端末が送信を許可されている、前記組織内ネットワーク外の送信先の送信許可リストと、

前記送受信端末が送信しようとするデータを暗号化する手段と、

前記送受信端末が送信しようとするデータを受信する手段と、前記送信許可リ

ストを参照して、前記データの送信の可否を決定する手段と、許可された場合に前記データを暗号化する手段と、前記暗号化データを、前記組織内ネットワーク外へ送信する手段を備える
送信制御可能なネットワークシステム。

【請求項９】

請求項１記載の送信制御可能なネットワークシステムであって、前記中継装置は、

前記組織内ネットワーク外から前記送受信端末へ向けて送信されてきた情報本体を受信する手段と、

前記情報本体に付加情報を取りつけ、前記データを生成する手段と、

前記データを前記送受信端末に送信することを特徴とする、送信制御可能なネットワークシステム。

【請求項１０】

請求項１記載の送信制御可能なネットワークシステムであって、前記送受信端末は、

各情報本体に付加すべき付加情報を記録した付加情報リストと、前記付加情報をデータの送信時とリムーバブルメディアへの書き込み時に前記情報本体に付加し、データを生成する手段を備える
送信制御可能なネットワークシステム。

【請求項１１】

請求項１記載の送信制御可能なネットワークシステムであって、

前記付加情報は前記情報本体の機密レベルを表す情報と、前記情報本体の特徴値と、前記機密レベルを表す情報と前記特徴値に対する第１のディジタル署名と、前記機密レベルを表す情報と前記情報本体に対する第２のディジタル署名とから成る
送信制御可能なネットワークシステム。

【請求項１２】

請求項１記載の送信制御可能なネットワークシステムであって、

前記送受信端末は、第１のＯＳと第２のＯＳと前記第１のＯＳと第２のＯＳを

制御する複数ＯＳ制御プログラムとを備え、

前記第１のＯＳは前記情報本体を扱うアプリケーションプログラムを管理し、

前記第２のＯＳは前記付加情報を用いた前記情報本体へのアクセス制御手段と、前記付加情報を変更する手段とを管理する

送信制御可能なネットワークシステム。

【請求項１３】

第1の記憶装置とリムーバブルメディアを読み書きする第２の記憶装置と、前記第1、第２の記憶装置へのアクセス手段と、各情報本体に付加すべき付加情報のリストである付加情報リストを備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、前記第１の記憶装置内の情報本体を前記第２の記憶装置へ記録する記録手段を備え、

前記記録手段は、前記付加情報リストに記録されている前記情報本体の付加情報を参照して前記データの暗号化の可否を決定する手段と、暗号化可能な場合に暗号化鍵を生成する手段と、前記暗号化鍵を用いて前記データを暗号化する手段と、前記鍵管理装置に前記暗号化鍵を登録する手段と、前記鍵管理装置から登録した前記暗号化鍵の識別子を受信する手段と、前記情報本体に前記付加情報を付加しデータを生成する手段と、前記データを前記暗号化鍵を用いて暗号化したデータと前記識別番号を第2の記憶装置へ記録する手段とを備える、送信制御可能なネットワークシステム。

【請求項１４】

第1の記憶装置とリムーバブルメディア対応の第２の記憶装置と、前記第1、第２の記憶装置へのアクセス手段と各情報本体に付加すべき付加情報のリストである付加情報リストを備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、第２の記憶装置内のデータを第１の記憶装置へ記録する記録手段を備え、

前記データは識別子と暗号化データを有し、

前記暗号化データは付加情報部を有し、

前記記録手段は、前記識別子を前記鍵管理装置に送信し、対応する前記暗号化データの暗号化鍵を受信する手段と、

前記暗号化データを前記暗号化鍵を用いて復号化する手段と、前記付加情報を前記付加情報リストに追加する手段とを備え、

前記鍵管理装置は、前記記録手段から前記識別子を受信し、対応する前記暗号化データの暗号化鍵を前記記録手段に送信する手段を備える

送信制御可能なネットワークシステム。

【請求項１５】

第1の記憶装置とリムーバブルメディアを読み書きする第２の記憶装置と、前記第1、第２の記憶装置へのアクセス手段を備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、前記第１の記憶装置内のデータを前記第２の記憶装置へ記録する記録手段を備え、

前記データは情報本体と前記情報本体に関連した付加情報とからなり、

前記記録手段は前記付加情報に基づき前記データの暗号化の可否を決定する手段と、暗号化鍵を生成する手段と、前記暗号化鍵を用いて前記データを暗号化する手段と、前記鍵管理装置に前記暗号化鍵を登録する手段と、前記鍵管理装置から登録した前記暗号化鍵の識別子を受信する手段と、前記暗号化したデータと前記識別子とを第2の記憶装置へ記録する手段と、を備え、

前記鍵管理装置は、前記記録手段から前記暗号化鍵を受信し、対応する前記識別子を前記記録手段に送信する手段を備える

送信制御可能なネットワークシステム。

【請求項１６】

第1の記憶装置とリムーバブルメディアを読み書きする第２の記憶装置と、前記第1、第２の記憶装置へのアクセス手段を備える情報処理装置と、暗号化鍵を管理する鍵管理装置を有する送信制御可能なネットワークシステムであって、

前記アクセス手段は、前記第２の記憶装置内のデータを前記第１の記憶装置へ記録する記録手段を備え、

前記データは識別子と暗号化データを有し、

前記記録手段は前記識別子を前記鍵管理装置に送信し、前記暗号化データの暗号化鍵を受信する手段と、前記暗号化データを前記暗号化鍵を用いて復号化する手段を備え、

前記鍵管理装置は、前記記録手段から前記識別子を受信し、対応する前記暗号化データの暗号化鍵を前記記録手段に送信する手段を備える

送信制御可能なネットワークシステム。

【請求項１７】

請求項４記載の送信制御可能なネットワークシステムであって、

前記送受信端末は、前記付加情報の変更手段を有し、

前記変更手段は、前記付加情報のデータの機密レベルと前記機密レベルの設定者情報と前記設定者の階級情報と、前記データの付加情報を変更しようとする者の変更者情報と前記変更者の階級情報とを参照し、前記データの機密レベルの変更の可否を決定する

送信制御可能なネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は組織などで扱う機密情報が外部に漏洩することを防止するための技術に関する。

【０００２】

【従来の技術】

企業などで扱う電子データには多くの社外秘情報が含まれる。これらの電子データには、意図的に文書内に「社外秘」と書き込むことによって閲覧者にその電子データが社外秘であることを伝える。外部に漏らさないように意識させることによって、社外秘データが外部に漏れることを防止している。しかしながら、ときには社外秘データを不注意または意図的にメールで外部に送信してしまう可能性がある。これらの問題に対して、サーバ側でメールの内容をキーワード検索することにより、社外秘情報と思われるあらかじめ設定したキーワード（例：社外秘）が含まれていないかどうかのチェックを行うことにより、そのキーワードが

含まれていない場合には、そのまま送信を行い、含まれている場合には送信を停止する。

【０００３】

また、企業内においても幹部しか参照することができない機密情報といったものが存在する。この機密情報が権限のない社員に参照されないように、強制アクセス制御機能を付加することにより、そのような機密情報が一般社員に参照されないように情報フロー制御を行うことが可能である。

【０００４】

強制アクセス制御については、文献[TCSEC]：「Department of Defense Trusted Computer System Evaluation Criteria」アメリカ国防総省標準（DOD 5200.28-STD）に詳しい。

また、従来、ネットワーク環境におけるマルチレベルセキュリティを実現するための技術として、米国特許5,940,591がある。

また、データを暗号化して送信することにより、機密情報の第３者への漏洩を防止する方法が、特開平8-204701号公報に開示されている。

【０００５】

【発明が解決しようとする課題】

キーワード検索に基づく情報漏洩を防止するシステムの場合、特定のデータフォーマットに対して有効であるが、未対応のデータフォーマットや文書情報が含まれない画像ファイルなどに対しては有効ではない。

【０００６】

また、強制アクセス制御機能を備える計算機の場合、その計算機内では十分な情報フロー制御を行うことは可能であるが、別の計算機にデータが移動した場合には、移動先の計算機のシステムに依存する為、データの機密レベルを保証することが困難となる。また、強制アクセス制御機能を備える計算機は特殊用途向けに利用されることが多く、汎用のアプリケーションを利用できないため、一般の企業や組織には普及しずらい。

【０００７】

また、上記米国特許5,940,591号では、（１）ユーザ単位のアクセス制御は提

供されているもののファイル単位のアクセス制御は行えない、（２）送信のたびにSMへの問い合わせが必要になり負荷が高い、などの課題がある。

【０００８】

また、データを暗号化して送信する場合、データを暗号化するのは社員の端末側であり、社員がどのデータが社外秘情報であるということを知っている必要がある。その為、不注意に社外秘データを暗号化せずに送信してしまう恐れがある。

【０００９】

【課題を解決するための手段】

本発明は、データの送信者の不注意により組織内の機密情報が外部へ送信されるのを防止する技術を提供する。

本発明は、上記技術を任意のデータフォーマットに対して適用可能なシステムを提供する。

本発明は、また、組織内でのデータの移動においてもデータの機密レベル（機密、非機密）を維持するとともに、それを任意のデータフォーマットに対して適用可能な技術を提供する。

【００１０】

具体的には、情報本体(データ本体)に、情報本体の属性を表す付加情報を付加し、付加情報を用いて、情報本体の送受信を制御する。

より具体的には、各データ本体(情報本体)に、属性を表すラベル（付加情報）をデータ本体に付加し、組織内ではラベル付きのデータを扱うようにする。属性としては、例えば機密レベル（社外秘、一般など）がある。外部へデータを送信する場合には、ゲートウェイサーバ上の送信管理プログラムがこのラベルをチェックし、外部へ送信してよいかどうかを決定し、外部へ送信可能であれば、データに付加されているラベルを取り除いて、データ本体を外部へ送信する。また、ゲートウェイサーバは外部からデータ本体を受信した場合には、データ本体にラベルを取りつけ、組織内のデータの送信先にデータを送信する。

【００１１】

また、ユーザが利用する端末においては、データ本体に直接ラベルを付加する

のではなく、各データの機密レベル情報を別のファイルに書き込んでも良い。クライアント端末からデータ本体を送信する時に上記ファイルを参照し、データ本体の機密レベルを表すラベルを付加し、ラベル付きのデータを送信すればよい。

また、ラベルに署名をつけることによって、ラベルを不正に改ざんされる恐れを防止することができ、さらに、誰が機密レベルを設定したかを保証することが可能となる。

【００１２】

また、本発明は、アプリケーションプログラムとデバイスドライバのバグ、さらにはユーザの操作ミスによるラベルの不正な変更や破壊を防止する技術を提供する。具体的には複数OS制御技術を用いて、２つのOSを動作させ、一方のOSをユーザが利用可能とし、もう一方のOSはラベル管理専用として用いる。

【００１３】

本発明によれば、上記米国特許と比較して、（１）アクセス制御リストによりデータ単位のアクセス制御が可能である、（２）アクセス制御リストは各ユーザ端末内にあるため毎回の問い合わせは不要、といった特徴を備える。

【００１４】

【発明の実施形態】

（第１の実施例）

本発明の第１の実施形態を説明する。本実施例では、ファイルに格納されたデータの先頭には機密レベルを表すラベルが付いており、このラベル情報を利用して、情報フロー制御を行う。機密レベルの内容やレベル数は、システムごとに自由に設定できるが、以下では「社外秘」「一般」の２段階の場合について説明する。なお、このラベルはファイルによって、ラベルを付けたり付けなかったりしても良い。例えば、システムファイル、ドライバファイルにはラベルを付けずに、アプリケーションのデータファイルにラベルを付ける。ラベルが付いていないファイルの取り扱いは、システムのポリシーとしてあらかじめ決めておく。本実施例において、ラベルが付いていないファイルは、クライアント端末側では「一般」のデータとして扱うものとする。

【００１５】

図１は本実施例のシステムの構成例である。１つ以上のクライアント端末１０１とゲートウェイサーバ１１８と鍵管理サーバ１１４が組織内ネットワーク１１７に繋がっており、さらに、ゲートウェイサーバ１１８は組織外ネットワーク１２１に繋がっている。クライアント端末１０１には、CPU１１３、メモリ１０２、磁気ディスク１０６、ネットワークI/F１１２、外部記憶装置１２２がある。メモリ１０２上には、ラベル管理プログラム１０９、ファイルシステムドライバ１０４、ディスクドライバ１０５、プロトコルドライバ１１０、ネットワークアダプタドライバ１１１、アプリケーションプログラム１０３、機密レベル変更プログラム１０８がロードされている。上記各プログラムは、OS(Operating System)の管理のもとで動作する。

【００１６】

磁気ディスク１０６内には複数のファイル１０７が格納されている。外部記憶装置１２２は、取り外し可能な記憶媒体（以下、リムーバブルメディアという）１２３内のファイル１２４からデータを読み取ったり、書き込んだりする装置である。外部記憶装置としては、例えば、フロッピーディスクドライブやCD-ROM装置などがある。ゲートウェイサーバ１１８には、送信管理プログラム１１９と受信管理プログラム１２０が動作している。鍵管理サーバ１１４には、鍵情報１１６があり、さらに鍵管理プログラム１１５が動作している。クライアント端末１０１はラベル付きファイルをネットワーク上に送信し、ゲートウェイサーバ１１８は当該ラベル付きファイルのラベルのチェックを行い、外部に当該ラベル付きファイルを送信してよいかどうかを決定する。

【００１７】

各実施例における各プログラムは、磁気ディスク１０６や、リムーバブルメディアや、組織内、組織外ネットワークに接続された他のサーバから、メモリ１０２に導入されても良い。

【００１８】

図２は、本実施例におけるラベルのフォーマットを例示している。ラベルはファイル１０７の先頭にあり、３２ビット（４バイト）の情報をもつ。３２ビットうちの最初の２ビットがラベルのフォーマットのバージョン情報２０１を表し、

次の３ビットがファイル１０７の機密レベル２０２を表し、次の3ビットがファイル１０７の機密レベルを設定した設定者レベル２０３を表し、残りの２４ビットがファイル１０７の機密レベルを設定した設定者ＩＤ２０４を表す。機密レベル２０２は、「一般」「社外秘」などであり、設定者レベル２０３は、例えば「社員」「係長」「課長」「部長」などである。なお、ラベルは機密レベル２０２の数や組織の規模、さらにその他の情報を付加したい場合など、組織によって異なるフォーマット、サイズにしても良い。その他の情報としては、例えば、ラベルの有効期限やファイル１０７の作成者情報、アクセス制御情報（読み取り専用など）がある。機密レベル２０２を用いるのではなく、その他の様々な情報を用いたアクセス制御を行ってもよい。

【００１９】

ラベル管理プログラム１０９は、ファイル１０７のラベルの管理を行い、アプリケーションプログラム１０３がファイル１０７にアクセスする場合にはラベルを取り外し、ラベル以外のデータ(データ本体)をアプリケーションプログラム１０３に渡す。また、アプリケーションプログラム１０３がファイル１０７をネットワークI/F１１２を介して組織内ネットワーク１１７上に送信する場合には、ラベル管理プログラム１０９はラベルが付いた状態で送信を行う。

【００２０】

図３は、本実施例における磁気ディスク１０６上にあるファイル１０７のオープンの処理フロー図である。ファイルのオープンとは、ファイル内のデータの読み取り、またはファイル内へのデータの書き込みなどの操作を可能にするための前処理である。

ステップ３０１では、アプリケーションプログラム１０３がファイル１０７のオープン要求をOSのI/Oマネージャを通じてラベル管理プログラム１０９に出す。

ステップ３０２では、ラベル管理プログラム１０９はアプリケーションプログラム１０３のプロセスIDをI/Oマネージャを通じて取得する。プロセスとは、OSが管理するプログラムの実行単位であり、プロセスIDはプロセスの識別子である。

【００２１】

ステップ３０３では、ラベル管理プログラム１０９は当該ファイル１０７の機密レベル２０２をチェックする。当該ファイル１０７にラベルが付いていない場合には、当該ファイル１０７は「一般」であると判断する。ラベルが付いていない例としては、システムファイル、ドライバファイルなどがある。

ステップ３０４では、ラベル管理プログラム１０９はプロセスIDからアプリケーションプログラム１０３の機密レベルをチェックする。ラベル管理プログラム１０９は、図４に示すプロセス管理リスト４００を参照することにより、アプリケーションプログラム１０３の機密レベルを調べる。アプリケーションプログラム１０３がファイル１０７をオープンしていない時点でのアプリケーションプログラム１０３の機密レベルは未設定となっている。

【００２２】

アプリケーションプログラムの機密レベル（実行中のプロセスの機密レベル）の必要性は次の通り。アプリケーションプログラム１０３そのものは、様々な機密レベルのファイルを扱うことができる。機密ファイルと非機密ファイルを同時に扱っている場合、機密情報が非機密ファイルの中に書き込まれてしまうことがあり得る（例えば、カット＆ペーストなど）。本実施例においては、プロセスの機密レベルを利用することにより、このような危険を防止する。

【００２３】

図４はプロセス管理リスト４００を表している。１列目にプロセスID４０１、２列目に当該プロセス機密レベル４０２（アプリケーションプログラムの機密レベル）、３列目にオープンしているファイル名４０３、４列目に当該ファイル１０７の機密レベル４０４が示されている。プロセス管理リスト４００は、ラベル管理プログラム１０９のロード時にラベル管理プログラム１０９が作成し、初期化を行う。また、ラベル管理リスト４００の更新もラベル管理プログラム１０９が行う。

【００２４】

続いて、ステップ３０５では、ラベル管理プログラム１０９はアプリケーションプログラム１０３の機密レベル４０２が設定済みであるかどうかチェックし、

設定済みである場合にはステップ３１１へ進み、未設定の場合にはステップ３０６へ進む。

ステップ３０６では、ラベル管理プログラム１０９はアプリケーションプログラム１０３のプロセスIDをプロセス管理リスト４００に追加する。

ステップ３０７では、ラベル管理プログラム１０９はアプリケーションプログラム１０３のプロセス機密レベル４０２を当該ファイル１０７の機密レベル２０２に設定する。

ステップ３０８では、ラベル管理プログラム１０９はプロセス管理リスト４００に当該ファイル１０７のファイル名４０３と機密レベル２０２を追加する。

ステップ３０９では、ラベル管理プログラム１０９は当該ファイル１０７のオープン要求をファイルシステムドライバ１０４に送信する。

ステップ３１０でファイルオープン成功となる。

【００２５】

ステップ３１１では、ラベル管理プログラム１０９はアプリケーションプログラム１０３の機密レベル４０２が当該ファイル１０７の機密レベル２０２と一致しているかどうかをチェックする。一致している場合にはステップ３０８へ進み、一致していない場合にはステップ３１２へ進む。

ステップ３１２では、ラベル管理プログラム１０９は当該ファイル１０７を本当にオープンするかどうかを利用者に選択させる為のメッセージを表示する。

ステップ３１３では、利用者がファイル１０７をオープンするかどうかの選択を行い、利用者がファイル１０７をオープンする、を選択した場合にはステップ３１４へ進み、利用者がファイル１０７をオープンしない、を選択した場合にはステップ３１５へ進む。

【００２６】

ステップ３１４では、ラベル管理プログラム１０９はアプリケーションプログラム１０３の機密レベル４０２が当該ファイル１０７の機密レベル２０２より高いかどうかのチェックを行い、アプリケーションプログラムの機密レベル４０２の方が高い場合にはステップ３０８へ進み、低い場合にはステップ３０７へ進む。

ステップ３１５では、ラベル管理プログラム１０９は当該ファイル１０７のオープンエラーメッセージをアプリケーションプログラム１０３に送信する。

ステップ３１６でファイルオープン失敗となる。

【００２７】

本実施例は、ユーザの指定次第でアプリケーションプログラム１０３が必ずファイル１０７をオープンすることが可能なように構成しているが、図３のステップ３１１において、アプリケーションプログラム１０３の機密レベル４０２がファイル１０７の機密レベル２０２と一致していない場合には、ステップ３１５に進み、ファイルオープン要求を強制的に拒否するように構成しても良い。

【００２８】

また、ファイルの新規作成時には、当該ファイルの機密レベル２０２を利用者が選択する形式をとる。標準設定では、アプリケーションプログラム１０３の機密レベル４０２と等しくなるようにし、アプリケーションプログラム１０３の機密レベル４０２が「未設定」の場合には、最上位の「社外秘」が選ばれるようにすることが望ましい。

【００２９】

図５は、本実施例におけるファイル１０７からデータを読み取る場合の処理フロー図である。ここでは例としてアプリケーションプログラム１０３がファイル１０７の先頭からのアドレスであるバイトオフセット0xAB00を読み取る場合について記述する。0xは16進数を示す。

ステップ５０１では、アプリケーションプログラム１０３がファイル１０７のバイトオフセット0xAB00からデータを読み取る要求を出す。

ステップ５０２では、ラベル管理プログラム１０９がバイトオフセット0xAB00を実際のバイトオフセット0xAB04に変換する。本実施例のファイル１０７はファイル１０７の先頭に４バイト（３２ビット）の情報（ラベル）が付いているが、アプリケーションプログラム１０３はラベルがあることを知らないため、アプリケーションプログラム１０３が読み取りを要求するバイトオフセットを調整する必要がある。そのため、本実施例ではアプリケーションプログラム１０３が要求するバイトオフセットにラベル情報のバイト長である４バイトを追加した値が実

際のバイトオフセットとなる。

ステップ５０３では、ファイルシステムドライバ１０４は実際のバイトオフセット0xAB04を磁気ディスク１０６上の相対位置に変換する。

ステップ５０４では、ディスクドライバ１０５は磁気ディスク１０６の相対位置を物理的な位置に変換してデータをメモリ１０２に読み込む。

【００３０】

図６は、本実施例におけるファイル１０７へデータを書き込む場合の処理フロー図である。ここでは例としてアプリケーションプログラム１０３がファイルの特定のバイトオフセット0xAB00に書き込む場合について記述する。

ステップ６０１では、アプリケーションプログラム１０３がファイル１０７のバイトオフセット0xAB00にデータを書き込む要求を出す。

ステップ６０２では、ラベル管理プログラム１０９はアプリケーションプログラム１０３の機密レベル４０２と当該ファイル１０７の機密レベル２０２をチェックする。

ステップ６０３では、ラベル管理プログラム１０９はアプリケーションプログラム１０３と当該ファイル１０７の機密レベルが一致しているかどうかをチェックし、一致している場合にはステップ６０５へ進み、一致していない場合にはステップ６０４へ進む。

【００３１】

ステップ６０５では、ラベル管理プログラム１０９がバイトオフセット0xAB00を実際のバイトオフセット0xAB04に変換する。上述したアプリケーションプログラム１０３がファイル１０７のデータを読み込む場合と同様、アプリケーションプログラム１０３が要求するバイトオフセットに４バイト追加した値が実際のバイトオフセットとなる。

ステップ６０６では、ファイルシステムドライバ１０４は実際のバイトオフセット0xAB04を磁気ディスク１０６上の相対位置に変換する。

ステップ６０７では、ディスクドライバ１０５は磁気ディスク１０６の相対位置を物理的な位置に変換してデータを磁気ディスク１０６に転送する。

【００３２】

ステップ６０４では、ラベル管理プログラム１０９は当該ファイル１０７の機密レベル２０２をアプリケーションプログラム１０３の機密レベル４０２に変更し、さらに、設定者レベル２０３、設定者ID２０４についても変更し、ステップ６０５へ進む。本実施例では、ステップ６０４で強制的にアプリケーションプログラム１０３の機密レベル４０２にファイル１０７の機密レベル２０２を変更したが、利用者がファイル１０７の機密レベル２０２を選択できるようにメッセージを表示しても良い。

【００３３】

本実施例のクライアント端末１０１には、外部記憶装置１２２があり、リムーバブルメディア１２３を用いてデータを別の端末に移動することができる。そのため、リムーバブルメディアを介して外部へ情報が漏洩するおそれがあるため、リムーバブルメディア１２３内のデータを外部の不正アクセスから保護する必要がある。

【００３４】

図７は、本実施例におけるリムーバブルメディア１２３へのファイル１０７の書き込みの処理フロー図である。ここでは、アプリケーションプログラム１０３が新規にファイル１２４を作成し、作成したファイル１２４にファイル１０７のデータをコピーする場合を説明する。ファイル１２４の機密レベルは、アプリケーションプログラム１０３が、ファイル１２４にデータを書き込む際に設定する。

【００３５】

ステップ７０１では、アプリケーションプログラム１０３がリムーバブルメディア１２３内のファイル１２４にファイル１０７のデータを書き込む要求を出す。

ステップ７０２では、ラベル管理プログラム１０９はファイル１０７の機密レベル２０２をチェックする。

ステップ７０３では、当該ファイル１０７の機密レベル２０２が「社外秘」であるかどうかを確認し、機密レベル２０２が「一般」の場合にはステップ７０４へ進み、「社外秘」の場合にはステップ７０６へ進む。

【００３６】

機密レベル２０２が「一般」の場合、ステップ７０４において、ラベル管理プログラム１０９はリムーバブルメディア１２３内のファイル１２４へ当該ファイル１０７のラベル以外のデータを書き込む要求を出す。

ステップ７０５では、ファイルシステムドライバ１０４が書き込み要求を受け取り、ディスクドライバ１０５がリムーバブルメディア１２３へ当該ファイル１０７のデータを転送する。

【００３７】

機密レベル２０２が「社外秘」の場合、ステップ７０６においては、ラベル管理プログラム１０９は暗号化鍵と復号化鍵を生成する。暗号化鍵と復号化鍵は同一であっても良い。

ステップ７０７では、ラベル管理プログラム１０９は復号化鍵を鍵管理サーバ１１４に登録し、識別子(例えば、ID番号)を鍵管理サーバ１１４から受け取る。

ステップ７０８では、ラベル管理プログラム１０９は当該ファイル１０７を、暗号化鍵を用いて暗号化し、暗号化ファイルを作成する。暗号化ファイルはID番号と暗号化データとから成る。ID番号はラベル管理プログラム１０９が暗号化ファイルの作成時に付加する。

ステップ７０９では、ラベル管理プログラム１０９はリムーバブルメディア１２３内のファイル１２４へ暗号化ファイルのデータを書き込む要求を出し、ステップ７０５へ進む。

【００３８】

また、既存のファイル１２４のデータを更新する場合で、データが暗号化されている場合には、ラベル管理プログラム１０９は、ファイル１２４に含まれているID番号を鍵管理サーバ１１４に送信し、鍵管理サーバ１１４から暗号化鍵を受信する。ラベル管理プログラム１０９は受信した暗号化鍵を用いてデータを暗号化し、ファイル１２４に暗号化データを書き込む。

【００３９】

図８はリムーバブルメディア１２３内のファイル１２４からデータを読み取る場合の処理フロー図である。

ステップ８０１では、アプリケーションプログラム１０３が、ラベル管理プログラム１０９に対して、リムーバブルメディア１２３内のファイル１２４からデータを読み取る要求を出す。

ステップ８０２では、ラベル管理プログラム１０９は、ファイルシステムドライバ１０４に対して、リムーバブルメディア１２３内の当該ファイル１２４からデータを読み取る要求を出す。

ステップ８０３では、ファイルシステムドライバ１０４が読み取り要求を受け取り、ディスクドライバ１０５がリムーバブルメディア１２３内の当該ファイル１２４からデータを読み込む。

ステップ８０４では、ラベル管理プログラム１０９は、読み出されたデータを受け取り、当該データが暗号化されているかをチェックする。

ステップ８０５では、当該データが暗号化されていない場合にはステップ８０６へ進み、暗号化されている場合にはステップ８０７へ進む。

【００４０】

ステップ８０６では、ラベル管理プログラム１０９はアプリケーションプログラム１０３にデータを渡す。

ステップ８０７では、ラベル管理プログラム１０９は当該ファイル１２４のID番号を読み取る。

ステップ８０８では、ラベル管理プログラム１０９は当該ファイル１２４のID番号を鍵管理サーバ１１４に送信し、当該ファイル１２４の復号化鍵を受け取る。

ステップ８０９では、ラベル管理プログラム１０９は暗号化されているデータを、復号化鍵を用いて復号化し、ステップ８０６へと進む。

ステップ８０８でのクライアント端末１０１と鍵管理サーバ１１４間の通信はデータを暗号化しても良い。

【００４１】

リムーバブルメディア１２３上のファイル１２４のデータを磁気ディスク１０６のファイル１０７へコピーまたは移動する場合で、当該ファイル１２４にラベルが付いていない場合は、ラベル管理プログラム１０９は当該ファイル１２４に

「一般」のラベルを付けて、磁気ディスク１０６に保存する。

【００４２】

図９はアプリケーションプログラム１０３がファイルをネットワーク１１７上へ送信する際の処理フロー図である。

ステップ９０１では、アプリケーションプログラム１０３がファイルを伴った当該ファイルの送信要求を出す。

ステップ９０２では、ラベル管理プログラム１０９は当該ファイル１０７の機密レベル２０２を取得し、ラベル付きファイルの送信要求に変換する。アプリケーションプログラム１０３は、送信対象データとして、ラベル無しのファイルデータを出力する為、ラベル管理プログラム１０９がラベル付きファイルに変換する。

ステップ９０３では、プロトコルドライバ１１０がラベル付きファイルをパケットに分割し、パケットヘッダを作成する。

ステップ９０４では、ネットワークアダプタドライバ１１１はLANコントローラを経由して外部へ当該ファイル１０７を送信する。

【００４３】

次に、機密レベル変更プログラム１０８について説明する。機密レベル変更プログラム１０８は、ファイル１０７の機密レベル２０２を変更するためのプログラムである。図１０は「社外秘」であるファイル１０７を「一般」に変更する場合の処理フロー図である。

ステップ１００１では、機密レベル変更プログラム１０８がファイル１０７の機密レベル２０２を「社外秘」から「一般」に変更する要求を出す。

ステップ１００２では、ラベル管理プログラム１０９はファイル１０７のラベルを読み込み、設定者ID２０４を取得する。

ステップ１００３では、ステップ１００２で取得した設定者ID２０４と機密レベル２０２の変更者IDが一致しているかどうかを判定する。一致している場合には、ステップ１００４へ進み、一致していなければステップ１００５へ進む。

【００４４】

ステップ１００４では、ラベル管理プログラム１０９は当該ファイル１０７の

機密レベル２０２を「一般」に変更し、設定者ID２０４、設定者レベル２０３も同時に変更する。

ステップ１００５では、機密レベル２０２の変更者が機密レベル２０２を変更できる権限を持っているかどうかを判定する。権限を持っていればステップ１００４へ進み、持っていなければステップ１００６へ進む。

ステップ１００６では、ラベル管理プログラム１０９はエラーメッセージを機密レベル変更プログラム１０８に渡す。

【００４５】

ステップ１００５において、機密レベル２０２を変更できる権限とは、強制的に機密レベル２０２を変更できる権限のことである。この権限は、機密レベル２０２を変更しようとする者のレベルがファイル１０７の設定者レベル２０３よりも高い場合に変更可能であるように設定することも可能である。また、機密レベル２０２を変更できるレベルを与えられていても、すべてのファイル１０７の機密レベル２０２を無条件に変更することは許さず、設定者ID２０４によって変更できる場合と変更できない場合を設定することも可能である。また機密レベル２０２を変更できる権限のポリシーを組織毎に分けて設定しても良い。ここでは、機密レベル２０２を「社外秘」から「一般」に変更する場合について記述したが、機密レベル２０２が3以上の場合においても同様の手法により機密レベル２０２を下げることが可能である。

【００４６】

機密レベル変更プログラム１０８は、また、「一般」ファイル１０７を「社外秘」ファイル１０７に機密レベル２０２を上げる操作を行うことが可能である。機密レベル２０２を上げることによって、情報が漏れることはないという考えに従えば、機密レベル２０２を上げる操作は誰でも無条件に行うことが可能であるように設定しても良い。

【００４７】

送信管理プログラム１１９は、クライアント端末１０１が組織外ネットワーク１２１に送信しようとするファイル１０７のラベルをチェックし、当該ファイル１０７を送信してよいかどうかを決定する。図１１はラベルのチェックの処理フ

ロー図である。

ステップ１２０１では、ゲートウェイサーバ１１８は組織内のクライアント端末１０１から組織外ネットワーク１２１へ送信しようとするファイル１０７を受信する。

ステップ１２０２では、送信管理プログラム１１９は当該ファイル１０７のラベルが付いているかどうかを判定する。

ステップ１２０３では、ラベルが付いていればステップ１２０４へ進み、付いていなければステップ１２０９へ進む。

【００４８】

ステップ１２０４では、送信管理プログラム１１９は当該ファイル１０７の機密レベル２０２をチェックする。

ステップ１２０５では、当該ファイル１０７の機密レベル２０２が「一般」であればステップ１２０６へ進み、「一般」でなければステップ１２１１へ進む。

ステップ１２０６では、送信管理プログラム１１９は当該ファイル１０７のラベルを取り外す。

ステップ１２０７では、送信管理プログラム１１９は当該ファイル１０７を外部に送信する。

ステップ１２０８でファイル送信成功となる。

【００４９】

ステップ１２０９では、送信管理プログラム１１９は当該ファイル１０７が不正データであると判断し、エラーメッセージを送信元端末と、システム管理者が使用する装置に送る。

ステップ１２１０でファイル送信失敗となる。

ステップ１２１１では、送信管理プログラム１１９は当該ファイル１０７の機密レベル２０２が「社外秘」であるというメッセージを送信元端末に送る。

ステップ１２１２でファイル送信失敗となる。

【００５０】

ステップ１２０６において、ラベルを取り外す理由は、ラベルが解釈できるのは本実施例のシステムが導入されている他のシステムや端末に限られるからとい

うポリシーに従うためである。したがって、本実施例においては、外部へファイルを送信する場合にはラベルを取り外すようにしているが、他のポリシーに従えば、これに限定されるものではない。

【００５１】

また、本実施例では、組織外に送信されるデータについては、ゲートウェイサーバ１１８上で組織外ネットワーク１２１に送信してよいかどうか判定された後、ラベルの取り外しをおこなわれるため、組織外ネットワーク１２１においても、透過的に利用可能である。

【００５２】

また、ゲートウェイサーバ１１８上に送信先許可リストを設けることにより、この送信先許可リストに記載された送信先へファイル１０７を送信する場合には、機密レベル２０２が「社外秘」の場合でも外部にファイル１０７を送信しても良い。この場合、送信管理プログラム１１９はファイル１０７を暗号化し、ラベルを取り外さずに送信する。さらに、送信管理プログラム１１９は送信元、送信先、送信ファイルをログに記録しておく。暗号鍵は、リムーバブルメディアへのファイル１０７の書き込みの場合と同様に鍵管理サーバ１１４に登録する。この場合の送信するファイル１０７はID番号と暗号化データを持つ。

【００５３】

次に、ゲートウェイサーバ１１８が組織外ネットワーク１２１からファイル１０７を受信した場合の処理について説明する。

まず、ゲートウェイサーバ１１８は組織外ネットワーク１２１からクライアント端末１０１へ向けて送信してきたファイル１０７を受信する。

次に、受信管理プログラム１２０は当該ファイル１０７に「一般」のラベルを取りつける。また、設定者ID２０４はゲートウェイサーバ１１８のIDとし、設定者レベル２０３は最低レベルに設定する。

その後、受信管理プログラム１２０はクライアント端末１０１へ当該ファイル１０７を送信する。

【００５４】

また、受信管理プログラム１２０はラベル付きのファイル１０７を受信する機

能を備えていても良い。この場合、受信管理プログラム１２０はラベルが付いていることを確認したあと、当該ファイル１０７をクライアント端末１０１に送信する。

【００５５】

組織内ネットワーク１１７内の端末間（クライアント端末１０１間、クライアント端末１０１とゲートウェイサーバ１１８間など）は互いに認証を行ってもよい。端末（１０１、１１８、１１４）間の認証は、各端末がそれぞれ通信を許可している端末のMAC(Media Access Control)アドレス（またはIPアドレス）のリスト（通信許可リスト）を持ち、各端末はこの通信許可リストを参照して認証を行う。各端末は、互いの通信許可リストに通信相手のMACアドレス（またはIPアドレス）があった場合に限り、端末間の通信が可能となるように制御すればよい。また、端末間の認証を各端末が行うのではなく認証サーバを設けることにより、この認証サーバが端末間の通信の許可を決定してもよい。この場合、各端末は認証サーバを経由して別の端末と通信を行う。また、端末間の認証は、公開鍵暗号方式を用いても良い。

【００５６】

さらに、認証サーバは、クライアント端末１０１が組織内または組織外の相手と送受信する全ファイルについて、そのラベルのチェックを行ってもよい。企業内においては社員の役職、または部署によってアクセス可能なファイル１０７とそうでないファイル１０７が存在するが、このような場合においても認証サーバがラベルのチェックを行うことにより、情報フロー制御を行うことが可能である。

【００５７】

（第２の実施例）

本発明の第２の実施形態を説明する。第１の実施例では、ファイル１０７の機密レベル２０２を表すラベルをファイル１０７に付けていたが、本実施例ではクライアント端末１０１内のファイル１０７にはラベルを付けずに、クライアント端末１０１内に設定する機密レベル制御リスト１４００を用いて情報フロー制御を行い、ファイル１０７をクライアント端末１０１外に出す場合にラベルを付け

る。ファイル１０７をクライアント端末１０１外に出す場合のラベルのフォーマットは第1の実施形態と同様である。

【００５８】

図１２は、本実施例の機密レベル制御リスト１４００を表している。1列目にファイル名１４０１、２列目に当該ファイル１０７の機密レベル１４０２、３列目に当該ファイル１０７の設定者レベル１４０３、４列目に当該ファイル１０７の設定者ID１４０４が格納されている。

【００５９】

本実施例におけるアプリケーションプログラム１０３による磁気ディスク１０６内のファイル１０７へのアクセスについて説明する。第1の実施形態と異なり、本実施例のファイル１０７にはラベルが付加されていないので、アプリケーションプログラム１０３が要求するバイトオフセットに処理を施す必要はない。ファイル１０７の読み取りに関しては、ラベル管理プログラム１０９はアプリケーションプログラム１０３が要求するバイトオフセットをそのままファイルシステムドライバ１０４に渡す。

【００６０】

一方、ファイル１０７への書き込みに関しては、バイトオフセットの処理を除けば図６と同様の処理を行う。つまり、アプリケーションプログラム１０３によるファイル１０７への書き込み要求に対して、ラベル管理プログラム１０９がアプリケーションプログラム１０３の機密レベル４０２と当該ファイル１０７の機密レベル２０２が一致しているかどうかのチェックを行い、一致していない場合には当該ファイル１０７の機密レベル２０２を強制的にアプリケーションプログラム１０３の機密レベル４０２に設定し、一致している場合にはファイル１０７への書き込み要求をファイルシステムドライバ１０４に送信する。

【００６１】

図１３は、本実施例におけるリムーバブルメディア１２３のファイル１０７へのデータ書き込みの処理フロー図である。

ステップ１５０１では、アプリケーションプログラム１０３がリムーバブルメディア１２３内のファイル１２４にへファイル１０７のデータを書き込む要求を

出す。

ステップ１５０２では、ラベル管理プログラム１０９はファイル１０７の機密レベル２０２をチェックする。

ステップ１５０３では、機密レベル２０２が「社外秘」であるかどうかを確認し、機密レベル２０２が「一般」の場合にはステップ１５０４へ進み、「社外秘」の場合にはステップ１５０６へ進む。

【００６２】

機密レベル２０２が「一般」の場合ステップ１５０４では、ラベル管理プログラム１０９は当該ファイル１０７のリムーバブルメディア１２３内のファイル１２４へ当該ファイル１０７のデータを書き込む要求を出す。

ステップ１５０５では、ファイルシステムドライバ１０４が書き込み要求を受け取り、ディスクドライバ１０５がリムーバブルメディア１２３へ当該１０７のデータを転送する。

【００６３】

機密レベル２０２が「社外秘」の場合、ステップ１５０６において、ラベル管理プログラム１０９は当該ファイル１０７のラベル付きファイルを作成する。

ステップ１５０７では、ラベル管理プログラム１０９は暗号化鍵を生成する。

ステップ１５０８では、ラベル管理プログラム１０９は暗号化鍵を鍵管理サーバ１１４に登録し、ID番号をサーバから受け取る。

ステップ１５０９では、ラベル管理プログラム１０９は当該ファイル１０７のラベル付きファイルを、暗号化鍵を用いて暗号化し、暗号化ファイルを作成する。暗号化ファイルはID番号と暗号化データとから成る。ID番号はラベル管理プログラム１０９が暗号化ファイルの作成時に付加する。

ステップ１５１０では、ラベル管理プログラム１０９は当該ラベル付きファイルをリムーバブルメディア１２３内のファイル１２４へ暗号化ファイルのデータを書き込む要求を出し、ステップ１５０５へ進む。

【００６４】

本実施例におけるリムーバブルメディア１２３内にあるファイル１２４のデータの読み取りは、第１の実施例と同様であり、図８に従う。また、リムーバブル

メディア１２３上のファイル１２３の磁気ディスク１０６へのコピーまたは移動では、ラベル管理プログラム１０９は機密レベル制御リスト１４００に当該ファイル１２４のファイル名１４０１、機密レベル１４０２、設定者レベル１４０３、設定者ID１４０４を追加し、当該ファイル１２４を磁気ディスク１０６に保存する。

【００６５】

次に本実施例におけるクライアント端末１０１でのファイル送信の処理について図９を用いて説明する。

ステップ９０１では、アプリケーションプログラム１０３がファイル１０７の送信要求を出す。本実施例においては、ステップ９０２に進む前に、ラベル管理プログラム１０９は当該ファイル１０７の機密レベル２０２を取得し、ラベル付きファイルを作成する処理ステップを追加している。続く処理は第一の実施例と同様であり、ステップ９０２へ進み、ラベル管理プログラム１０９が当該ファイル１０７の送信要求を、当該ラベル付きファイル１０７の送信要求に変換する。

ステップ９０３では、プロトコルドライバ１１０はパケットに分割し、パケットヘッダを作成する。

ステップ９０４では、ネットワークアダプタドライバ１１１はLANコントローラを経由して外部へファイル１０７を送信する。

【００６６】

ファイル１０７の削除要求が発生した場合には、ラベル管理プログラム１０９は当該ファイル１０７の削除要求をファイルシステムドライバ１０４に送信し、ファイルシステムドライバ１０４から当該ファイル１０７の削除が成功したというメッセージを受け取ったあとで、ラベル管理プログラム１０９は機密レベル制御リスト１４００から当該ファイル１０７の行を削除する。

【００６７】

他のクライアント端末１０１、またはゲートウェイサーバ１１８からファイル１０７を受信した場合、ラベル管理プログラム１０９がファイル１０７の先頭に付いているラベルをチェックし、機密レベル制御リスト１４００にファイル１０７のラベル情報の登録を行う。その後、ラベル管理プログラム１０９はアプリケ

ーションプログラム１０３に当該ファイル１０７を渡す。

【００６８】

ファイル１０７の機密レベル２０２の変更は、ラベル管理プログラム１０９が機密レベル変更プログラム１０８から当該ファイル１０７の機密レベル２０２変更要求を受け取り、機密レベル制御リスト１４００を変更することにより行う。具体的には機密レベル制御リスト１４００を用いる点を除き、図１０の処理フローに従う。

【００６９】

第１の実施例または第２の実施例によれば、ファイル１０７に機密レベル２０２を設定し、ネットワークにおける情報フロー制御を行うことが可能となる。

【００７０】

（第３の実施例）

次に、ラベルの完全性を保証でき、ラベルの不正な改ざんを防止することが可能な、第３の実施形態を説明する。

【００７１】

本実施例によれば、第3者がラベルを不正に変更することにより、ラベルを実際に変更したのが誰であるかということを隠すという、更なる不正を防止することが可能になる。つまり、第３者Aが不正にラベルを改ざんし、例えば、「社外秘」レベルのファイル１０７を「一般」に変更し、さらに設定者IDを他人BのIDに設定することにより、Bが機密レベルを変更したことにする、といった不正を防止することが可能である。すなわち、万一、「社外秘」レベルのファイル１０７が社外に漏洩しても、覚えのないBが責任を追及される、といったことを防止できる。

【００７２】

図１４は、本実施例で用いるラベル付きファイル１０７の構造を表す図である。ラベル付きファイル１０７は、先頭にラベル１７０１があり、続いてデータハッシュ値１７０２、ラベル用署名１７０３、ファイルデータ１７０４、リンク用署名１７０５からなる。

【００７３】

データハッシュ値１７０２は、機密レベル２０２の設定者自身がファイル１０７を作成、または訂正、または機密レベル２０２を変更した時点でのファイルデータのハッシュ値である。ラベル用署名１７０３はラベル１７０１とデータハッシュ値１７０２とに対する機密レベル２０２の設定者によるディジタル署名である。リンク用署名１７０５はラベル１７０１とファイルデータ１７０４とに対するファイルデータ１７０４の作成者または変更者によるディジタル署名である。

【００７４】

ラベル用署名１７０３によってラベル１７０１の完全性を保証し、リンク用署名１７０５によってファイルデータ１７０４の完全性と、ファイルデータ１７０４とラベル１７０１とのリンクの完全性を保証する。ラベル用署名１７０３とリンク用署名１７０５を用いることは、万一、情報漏洩が起きた場合に責任の所在を調査する上で有効になるとともに、証拠が残るという意味で不正な情報漏洩を抑止する効果がある。なお、署名生成のための秘密鍵は利用者毎に異なる鍵を持っていることが望ましい。

【００７５】

なお、本実施例は第１の実施例の拡張として用いてもよく、その場合にはこのファイル構造をクライアント端末１０１内外で用いる。また、第２の実施例の拡張として用いる場合には、このファイル構造をクライアント端末１０１外で用いて、クライアント端末１０１内では、機密レベル制御リスト１４００にデータハッシュ値１７０２、ラベル用署名１７０３、リンク用署名１７０５の列を追加することによりラベル情報の完全性を保証する。

【００７６】

以下では、本実施例では第２の実施例を拡張した場合について説明する。

図１５は、本実施例でのファイル１０７へのデータ（ファイルデータ１７０４）の書き込みの処理フロー図である。

ステップ１８０１では、アプリケーションプログラム１０３がファイル１０７へデータ（ファイルデータ１７０４）の書き込み要求を出す。

ステップ１８０２では、ラベル管理プログラム１０９はアプリケーションプログラム１０３の機密レベル４０２と当該ファイル１０７の機密レベル２０２が一

致しているかをプロセス管理リスト４００と機密レベル制御リスト１４００を参照してチェックする。

ステップ１８０３では、アプリケーションプログラム１０３と当該ファイル１０７の機密レベル２０２が一致している場合にはステップ１８０６へ進み、一致していない場合にはステップ１８０４へ進む。

【００７７】

ステップ１８０４では、ラベル管理プログラム１０９は当該ファイル１０７の機密レベル２０２をアプリケーションプログラム１０３の機密レベル４０２に変更し、さらに、設定者レベル２０３、設定者ID２０４についても変更する。

ステップ１８０５では、ラベル管理プログラム１０９はデータハッシュ値１７０２、ラベル用署名１７０３、リンク用署名１７０５を、新たに求め、ステップ１８０８へ進む。ここで、データハッシュ値１７０２は変更後のファイルデータ１７０４のハッシュ値であり、ラベル用署名１７０３とリンク用署名１７０５はファイル１０７への書き込み要求者の署名である。

【００７８】

ステップ１８０６では、ラベル管理プログラム１０９は当該ファイル１０７の機密レベル２０２設定者とファイル１０７への書き込み要求者が一致しているかどうかをチェックし、一致している場合にはステップ１８０５へ進み、一致していない場合にはステップ１８０７へ進む。

ステップ１８０７では、ラベル管理プログラム１０９はリンク用署名１７０５を新たに求める。ここでリンク用署名１７０５はファイル１０７への書き込み要求者の署名である。

ステップ１８０８では、ラベル管理プログラム１０９はファイルシステムドライバ１０４に対して当該ファイル１０７へ、上記データハッシュ値１７０２、ラベル用署名１７０３、リンク用署名１７０５のうち新たに求めたものと、ファイルデータ１７０４の書き込み要求を出す。

ステップ１８０９では、ファイルシステムドライバは当該ファイルへ書き込むデータをディスクドライバに送信し、ディスクドライバは磁気ディスクに上記データを書き込む。

【００７９】

本実施例におけるクライアント端末１０１での上記ラベル付きファイル１０７の送信処理について説明する。まず、ラベル管理プログラム１０９がアプリケーションプログラム１０３からファイル送信要求を受け取る。次に、ラベル管理プログラム１０９はアプリケーションプログラム１０３からのファイル送信要求を当該ラベル付きファイル１０７の送信要求に変換する。具体的には、クライアント端末１０１から送信されるファイル構造は図１４に示す構造と同じである。

【００８０】

図１６は、本実施例でのクライアント端末１０１におけるファイル受信の処理フロー図である。

ステップ１９０１では、ラベル管理プログラム１０９はラベル付きファイル１０７を受信する。

ステップ１９０２では、ラベル管理プログラム１０９はラベル付きファイル１０７のラベル１７０１をチェックする。ここでは、ラベル管理プログラム１０９はラベル用署名１７０３からラベル１７０１の正当性を検証し、リンク用署名１７０５からファイルデータ１７０４の完全性と、ファイルデータ１７０４とラベル１７０１とのリンクの正当性をチェックする。

ステップ１９０３では、ステップ１９０２でのチェックの結果、ラベル１７０１、ファイルデータ１７０４、ファイルデータ１７０４とラベル１７０１とのリンクが正しい場合にはステップ１９０４へ進み、正しくない場合にはステップ１９０６へ進む。

【００８１】

ステップ１９０４では、ラベル管理プログラム１０９は当該ラベル付きファイル１０７のラベル情報を機密レベル制御リスト１４００に追加する。

ステップ１９０５では、ラベル管理プログラム１０９は当該ラベル付きファイル１０７をアプリケーションプログラム１０３に渡す。

【００８２】

ステップ１９０６では、ラベル管理プログラム１０９は当該ラベル付きファイル１０７のラベル情報を管理者に送信する。

ステップ１９０７では、ラベル管理プログラム１０９はエラーメッセージをアプリケーションプログラム１０３に送る。

【００８３】

次に、本実施例における「社外秘」であるラベル付きファイル１０７を「一般」に変更する場合の処理について図１０を参考に用いて説明する。。

ステップ１００１では、機密レベル変更プログラム１０８がラベル付きファイル１０７の機密レベル２０２を「社外秘」から「一般」に変更する要求を出す。

ステップ１００２では、ラベル管理プログラム１０９は、本実施例においては機密レベル制御リスト１４００から当該ラベル付きファイル１０７の設定者ID２０４を取得する。

ステップ１００３では、ステップ１００２で取得した設定者ID２０４と機密レベル２０２の変更者IDが一致しているかどうかを判定する。一致している場合には、ステップ１００４へ進み、一致していなければステップ１００５へ進む。

【００８４】

ステップ１００４では、ラベル管理プログラム１０９はラベル付きファイル１０７の機密レベル２０２を「一般」に変更し、設定者ID２０４、設定者レベル２０３も同時に変更する。本実施例においては、ラベル管理プログラム１０９は、さらに、ラベル用署名１７０３、リンク用署名１７０５を新たに求める処理を行う。

【００８５】

ステップ１００５以降の処理は第一の実施例と同様であり、ステップ１００５において、機密レベル２０２の変更者が機密レベル２０２を変更できる権限を持っているかどうかを判定する。権限を持っていればステップ１００４へ進み、持っていなければステップ１００６へ進む。

ステップ１００６では、ラベル管理プログラム１０９はエラーメッセージを機密レベル変更プログラム１０８に渡す。

【００８６】

上記実施例では、機密レベル２０２を「社外秘」から「一般」に変更する場合について記述したが、機密レベル２０２が３レベル以上の場合においても同様の

手法により機密レベル２０２を下げることが可能である。

【００８７】

図１７は、本実施例におけるゲートウェイサーバ１１８でのラベル１７０１のチェックの処理フロー図である。

ステップ２１０１では、組織内のクライアント端末１０１から外部へ送信するファイル１０７を受信する。

ステップ２１０２では、送信管理プログラム１１９は当該ファイル１０７のラベル１７０１の有無をチェックする。

ステップ２１０３では、ラベル１７０１が付いていればステップ２１０４へ進み、付いていなければステップ２１１１へ進む。

【００８８】

ステップ２１０４では、送信管理プログラム１１９は当該ラベル付きファイル１０７の機密レベル２０２をチェックする。

ステップ２１０５では、機密レベル２０２が「一般」であればステップ２１０６へ進み、「一般」でなければステップ２１１３へ進む。

【００８９】

ステップ２１０６では、送信管理プログラム１１９はラベル１７０１の完全性のチェックを行う。ここでは、送信管理プログラム１１９はラベル用署名１７０３からラベル１７０１の正当性を検証し、リンク用署名１７０５からファイルデータ１７０４の完全性と、ファイルデータ１７０４とラベル１７０１とのリンクの正当性をチェックする。

ステップ２１０７では、ステップ２１０６でのチェックの結果、リンクが正しい場合にはステップ２１０８へ進み、正しくない場合にはステップ２１１５へ進む。

【００９０】

ステップ２１０８では、送信管理プログラム１１９は当該ラベル付きファイル１０７からラベル１７０１、データハッシュ値１７０２、ラベル用署名１７０３、リンク用署名１７０５を取り外す。

ステップ２１０９では、送信管理プログラム１１９は当該ファイル１０７を外

部に送信する。

ステップ２１１０でファイル送信成功となる。

【００９１】

ステップ２１１１では、送信管理プログラム１１９は当該ファイル１０７が不正データであると判断し、エラーメッセージを送信元端末に送る。

ステップ２１１２でファイル送信失敗となる。

【００９２】

ステップ２１１３では、送信管理プログラム１１９は当該ラベル付きファイル１０７の機密レベル２０２が「一般」ではないというメッセージを送信元端末に送る。

ステップ２１１４でファイル送信失敗となる。

【００９３】

ステップ２１１５では、送信管理プログラム１１９は当該ラベル付きファイル１０７のラベルが不正であるというメッセージを送信元端末に送る。

ステップ２１１６でファイル送信失敗となる。

【００９４】

また、送信管理プログラム１１９は、ファイルの送信元情報と送信先情報と送信ファイル（ラベル１７０１、データハッシュ値１７０２、ラベル用署名１７０３、リンク用署名１７０５の付いたファイル）の内容全てをログに記憶しておいても良い。

【００９５】

本実施例において、ゲートウェイサーバ１１８が、組織外ネットワーク１２１からクライアント端末１０１へ向けて送信されてきたファイル１０７を受信した場合は、受信管理プログラム１２０がファイル１０７に「一般」のラベルを取りつけ、クライアント端末１０１へファイル１０７を送信する。ここで、ラベルの設定者ID２０４はゲートウェイサーバ１１８のIDとし、設定者レベル２０３は最低レベルに設定する。また、ラベル用署名１７０３とリンク用署名１７０５はゲートウェイサーバ１１８による署名にする。

また、受信管理プログラム１２０は、ファイル１０７の送信元情報と送信先情

報と受信ファイルの内容全てをログに記憶しておいても良い。

【００９６】

（第４の実施例）

本発明の第４の実施形態を説明する。

汎用の計算機上にはさまざまなアプリケーションプログラム１０３が動作しており、さらに、さまざまなデバイスが接続されており、そのデバイスを操作する為のデバイスドライバが動作している。その為、上記各実施例を汎用の計算機上で実現する場合、アプリケーションプログラム１０３とデバイスドライバのバグ、さらにはユーザの操作ミスによってラベル情報（機密レベル制御リスト１４００）、ラベル管理プログラム１０９、プロセス管理リスト４００が変更、削除される脅威がある。本実施例によれば、そのような脅威を防止することが可能である。

図１８は本実施例によるクライアント端末１０１の構成例であり、図１のクライアント端末１０１に置き換え、上記各実施例に適用することにより、上記効果を得ることができる。

【００９７】

クライアント端末１０１内には２つのOSが動作しており、第１のOSが管理するメモリ領域２２０１と第２のOSが管理するメモリ領域２２０２があり、さらにこれら２つのOSを制御する複数OS制御プログラム２２０４が動作している。複数OS制御技術に関しては、たとえば、特開平１１－１４９３８５号公報に開示されている。

【００９８】

また、第１のOSが管理するメモリ領域２２０１内には、アプリケーションプログラム１０３、機密レベル変更プログラム１０８、I/Oフックプログラム２２０３、ファイルシステムドライバ１０４、ディスクドライバ１０５、プロトコルドライバ１１０、ネットワークアダプタドライバ１１１がロードされており、また、第１のOSは磁気ディスク１０６、ネットワークI/F１１２を管理しており、磁気ディスク１０６内にはファイル１０７が格納されている。

【００９９】

第２のOSが管理するメモリ領域２２０２内には、ラベル管理プログラム１０９、プロセス管理リスト４００があり、また、第２のOSは磁気ディスク２２０５を管理しており、磁気ディスク２２０５内には機密レベル制御リスト１４００が格納されている。

【０１００】

I/Oフックプログラム２２０３はアプリケーションプログラム１０３または機密レベル変更プログラム１０８からのファイル１０７へのアクセス要求またはファイル１０７の送受信要求をフックする。さらに、I/Oフックプログラム２２０３はラベル管理プログラム１０９に処理を依頼する機能とラベル管理プログラム１０９の処理結果を受け取りファイルシステムドライバ１０４またはプロトコルドライバ１１０に処理結果を渡す機能を持っている。具体的にはI/Oフックプログラム２２０３は複数OS制御プログラム２２０４のOS間通信機能を利用してラベル管理プログラム１０９に処理を依頼する。OS間通信機能に関しては、たとえば、特開平１１－８５５４６号公報に開示されている。

【０１０１】

本実施例によれば、保護対象（ラベル管理プログラム１０９、プロセス管理リスト４００、機密レベル制御リスト１４００）を第２のOSが管理することにより、第１のOS上で動作しているアプリケーションプログラム１０３、デバイスドライバのバグまたはユーザの操作ミスによる変更から保護することが可能となる。

【０１０２】

（その他）

上記各実施例によれば、単に組織内の機密情報の漏洩を防止できるだけでなく、組織外ネットワーク１２１経由での不正侵入による機密情報の漏洩も防止することも可能になる。不正侵入者がゲートウェイサーバ１１８を経由してクライアント端末１０１内の機密ファイルを持ち出そうとした場合、ゲートウェイサーバ１１８の送信管理プログラム１１９は、当該機密ファイルのラベルをチェックする。機密レベルが「社外秘」の場合、送信管理プログラム１１９は外部への送信を拒否する為、機密ファイルの漏洩を防止することが可能である。

【０１０３】

また、信頼できない（Untrusted）プログラム（例：メールに添付されてくるプログラム）に対しては、ラベル管理プログラム１０９が「Untrusted」というラベルを取りつけ、アクセスできるファイルに制限を加えるように構成することも可能である。

具体的にはシステムファイルやカーネルの設定情報ファイルに「Trusted」のラベルを付け、「Untrusted」のプログラムが「Trusted」のファイルへアクセスした場合に、ラベル管理プログラム１０９がアクセス制限を加えるように構成すればよい。この機能は、たとえば、ファイルオープン時にラベル管理プログラム１０９がプログラムとファイルのラベルをそれぞれチェックすることにより実現可能になる。このような機能を用いれば、コンピュータウィルスによるシステムへの影響を最小限に抑えることが可能である。

【０１０４】

また、専用の通信プロトコルを用いて、クライアント端末１０１とゲートウェイサーバ１１８間の通信を行ってもよい。これにより、例えば、各パケットのヘッダ領域にラベルを付加し、ゲートウェイサーバ１１８の送信管理プログラム１１９はこのパケットのヘッダ領域のラベルをチェックすることによりデータの送信の可否を決定することが可能となる。専用の通信プロトコルを用いた場合はは、データを組織外ネットワーク１２１へ送信する場合には、送信管理プログラム１１９はラベルを取り除き、汎用の通信プロトコル（ＴＣＰ／ＩＰなど）のパケットに変換するように構成すればよい。

【０１０５】

また、電子メールの添付ファイルにラベル付きのファイル１０７を添付して送信し、ゲートウェイサーバ１２１では、メールの添付ファイルのラベルをチェックすることにより、電子メールによって機密ファイルが社外に漏洩することを防止することが可能である。なお、メール本文に関しては、キーワード検索によってポリシーに反するキーワードが含まれていないかどうかをチェックすることにより、漏洩防止が可能になる。

【０１０６】

また、クライアント端末１０１毎に機密レベルを設定し、さらにクライアント

端末１０１間と、クライアント端末１０１と各サーバ間に中間サーバを設け、中間サーバに情報漏洩防止機能を持たせても良い。この場合、クライアント端末１０１上のファイル１０７にはラベルを付けなくてもよい。

【０１０７】

この例において、中間サーバは各クライアント端末１０１の機密レベルを管理し、クライアント端末１０１が送信したファイル１０７を別のクライアント端末１０１あるいは他の部署あるいはグループに送信してよいかどうかを決定する。中間サーバはクライアント端末１０１に直接ファイル１０７を送信する場合にはラベルを取りつけず、他の部署あるいはグループの中間サーバに送信する場合にはラベルを取りつける。中間サーバは別の中間サーバから受信したファイル１０７のラベルをチェックし、クライアント端末１０１に送信する場合にはラベルを取り外してファイル１０７を送信する。なお、中間サーバは部署単位あるいはグループ単位に設けても良い。

【０１０８】

このようにすることにより、各クライアント端末１０７にはラベル管理プログラム１０９を組み込む必要がなくなり、情報漏洩防止機能を導入する為の手間を軽減できる。

【０１０９】

【発明の効果】

機密ファイルの漏洩を防止することが、任意のファイルフォーマットに対して対応可能なシステムを提供できる。

【０１１０】

【符号の説明】

１０１：クライアント端末、１０２：メモリ、１０３：アプリケーションプログラム、１０４：ファイルシステムドライバ、１０５：ディスクドライバ、１０６：磁気ディスク、１０７：ファイル、１０８：機密レベル変更プログラム、１０９：ラベル管理プログラム、１１０：プロトコルドライバ、１１１：ネットワークアダプタドライバ、１１２：ネットワークI/F、１１３：ＣＰＵ、１１４：鍵管理サーバ、１１５：鍵管理プログラム、１１６：鍵情報、１１７：組織内ネッ

トワーク、１１８：ゲートウェイサーバ、１１９：送信管理プログラム、１２０：受信管理プログラム、１２１：組織外ネットワーク、１２２：外部記憶装置、１２３：リムーバブルメディア、１２４：ファイル、２０１：バージョン情報、２０２：機密レベル、２０３：設定者レベル、２０４：設定者ＩＤ、４００：プロセス管理リスト、４０１：プロセスＩＤ、４０２：プロセス機密レベル、４０３：ファイル名、４０４：ファイルの機密レベル、１４００：機密レベル制御リスト、１４０１：ファイル名、１４０２：機密レベル、１４０３：設定者レベル、１４０４：設定者ＩＤ、１７０１：ラベル、１７０２：データハッシュ値、１７０３：ラベル用署名、１７０４：ファイルデータ、１７０５：リンク用署名、２２０１：第１のＯＳが管理するメモリ領域、２２０２：第２のＯＳが管理するメモリ領域、２２０３：I/0フックプログラム、２２０４：複数ＯＳ制御プログラム、２２０５：磁気ディスク。

【０１１１】

【図面の簡単な説明】

【図１】

本発明によるネットワークシステムの全体を表す図である。

【図２】

ラベルのフォーマットを表す図である。

【図３】

ファイルオープンの処理フロー図である。

【図４】

プロセス管理リストを表す図である。

【図５】

ファイルの読み取りの処理フロー図である。

【図６】

ファイルへの書き込みの処理フロー図である。

【図７】

リムーバブルメディアへのファイルの書き込みの処理フロー図である。

【図８】

リムーバブルメディアからのファイルの読み取りの処理フロー図である。

【図９】

ファイルのネットワーク上への送信の処理フロー図である。

【図１０】

機密レベルの変更の処理フロー図である。

【図１１】

ゲートウェイサーバでのラベルのチェックの処理フロー図である。

【図１２】

機密レベル制御リストのフォーマットを表す図である。

【図１３】

第２の実施例におけるリムーバブルメディアへのファイルの書き込みの処理フロー図である。

【図１４】

第３の実施例におけるラベル付きファイルの構造を表す図である。

【図１５】

第３の実施例におけるファイルへの書き込みの処理フロー図である。

【図１６】

クライアント端末におけるファイル受信の処理フロー図である。

【図１７】

第３の実施例におけるゲートウェイサーバでのラベルのチェックの処理フロー図である。

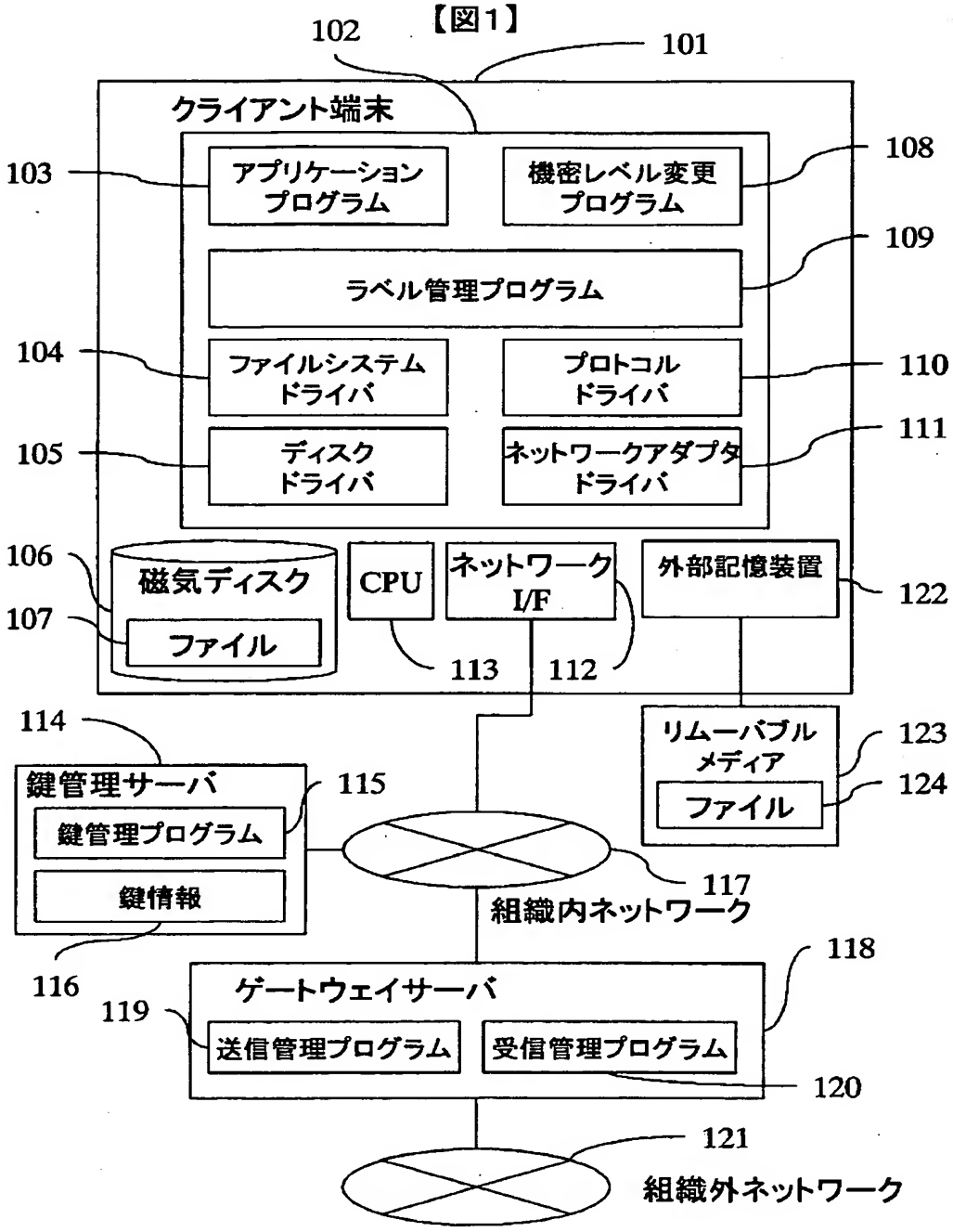
【図１８】

２つのＯＳを利用した本発明によるネットワークシステムのクライアント端末の構成図である。

【書類名】　図面

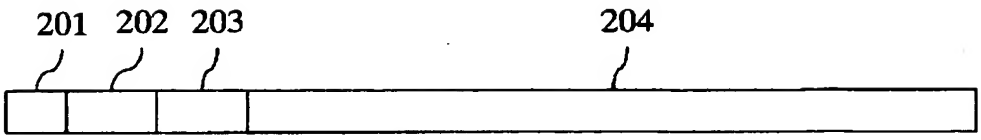
【図１】

【図1】


102
101
クライアント端末
103
アプリケーション
プログラム
機密レベル変更
プログラム
108
109
ラベル管理プログラム
104
ファイルシステム
ドライバ
プロトコル
ドライバ
110
105
ディスク
ドライバ
ネットワークアダプタ
ドライバ
111
106
磁気ディスク
107
ファイル
CPU
ネットワーク
I/F
外部記憶装置
122
113
112
114
リムーバブル
メディア
123
124
ファイル
鍵管理サーバ
115
鍵管理プログラム
鍵情報
117
組織内ネットワーク
116
118
ゲートウェイサーバ
119
送信管理プログラム
受信管理プログラム
120
121
組織外ネットワーク

【図２】

【図2】



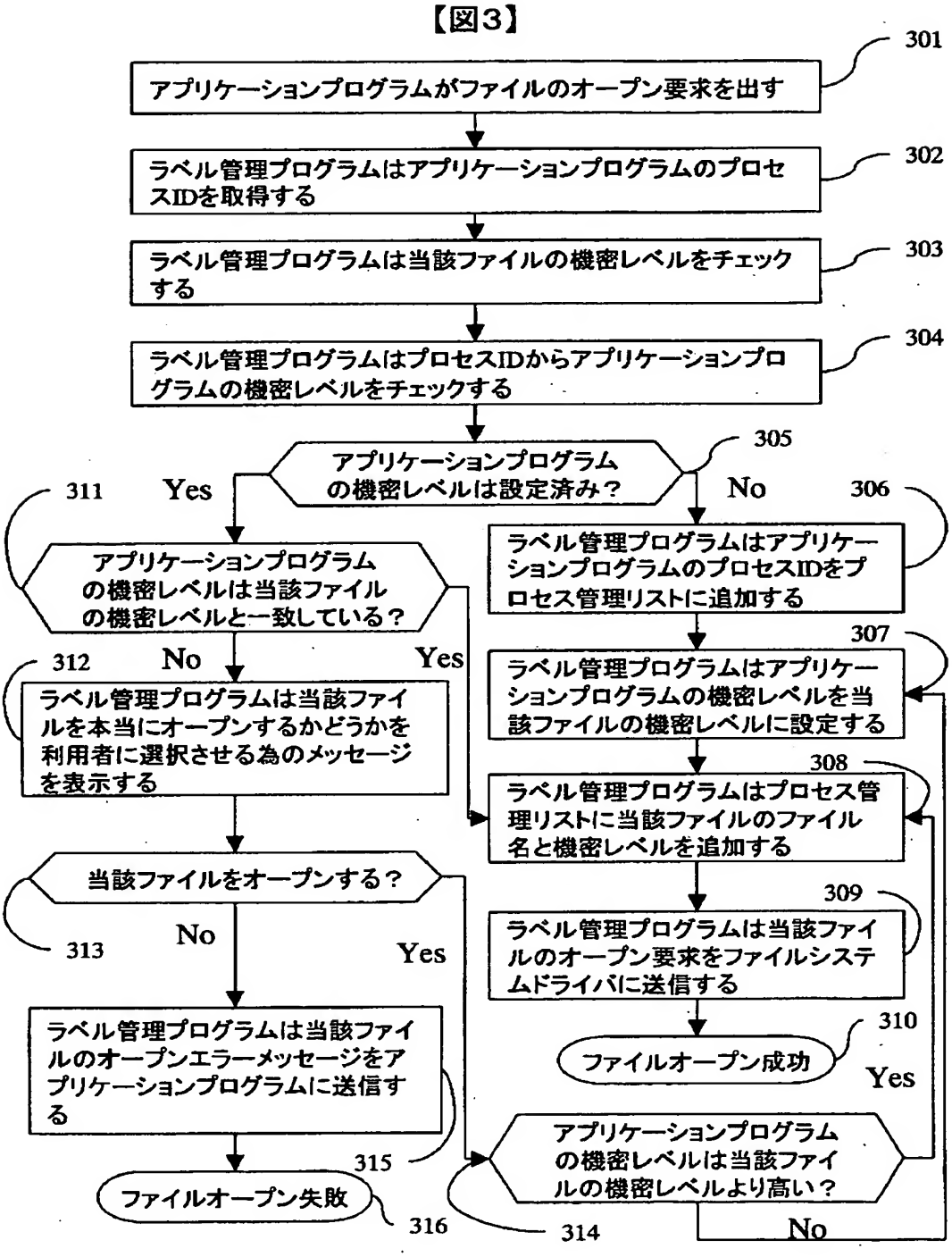
201: バージョン情報 (2bit)

202: 機密レベル (3bit)

203: 設定者レベル (3bit)

204: 設定者ID (24bit)

【図３】


【図3】
301
アプリケーションプログラムがファイルのオープン要求を出す
302
ラベル管理プログラムはアプリケーションプログラムのプロセスIDを取得する
303
ラベル管理プログラムは当該ファイルの機密レベルをチェックする
304
ラベル管理プログラムはプロセスIDからアプリケーションプログラムの機密レベルをチェックする
305
アプリケーションプログラムの機密レベルは設定済み？
Yes
No
311
306
ラベル管理プログラムはアプリケーションプログラムのプロセスIDをプロセス管理リストに追加する
アプリケーションプログラムの機密レベルは当該ファイルの機密レベルと一致している？
307
ラベル管理プログラムはアプリケーションプログラムの機密レベルを当該ファイルの機密レベルに設定する
312
No
Yes
ラベル管理プログラムは当該ファイルを本当にオープンするかどうかを利用者に選択させる為のメッセージを表示する
308
ラベル管理プログラムはプロセス管理リストに当該ファイルのファイル名と機密レベルを追加する
当該ファイルをオープンする？
309
No
313
Yes
ラベル管理プログラムは当該ファイルのオープン要求をファイルシステムドライバに送信する
310
ファイルオープン成功
Yes
ラベル管理プログラムは当該ファイルのオープンエラーメッセージをアプリケーションプログラムに送信する
315
アプリケーションプログラムの機密レベルは当該ファイルの機密レベルより高い？
ファイルオープン失敗
316
314
No

【図４】

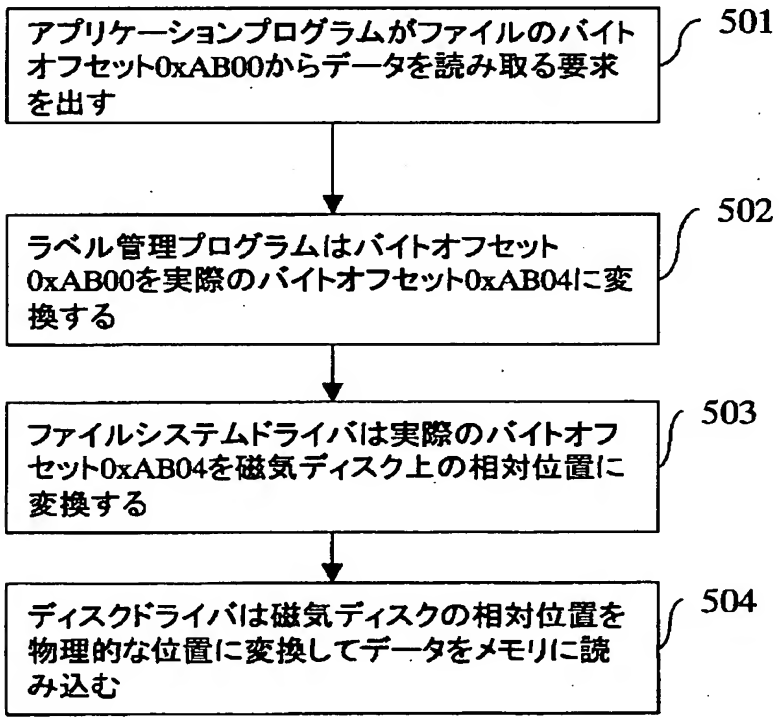
【図4】

400

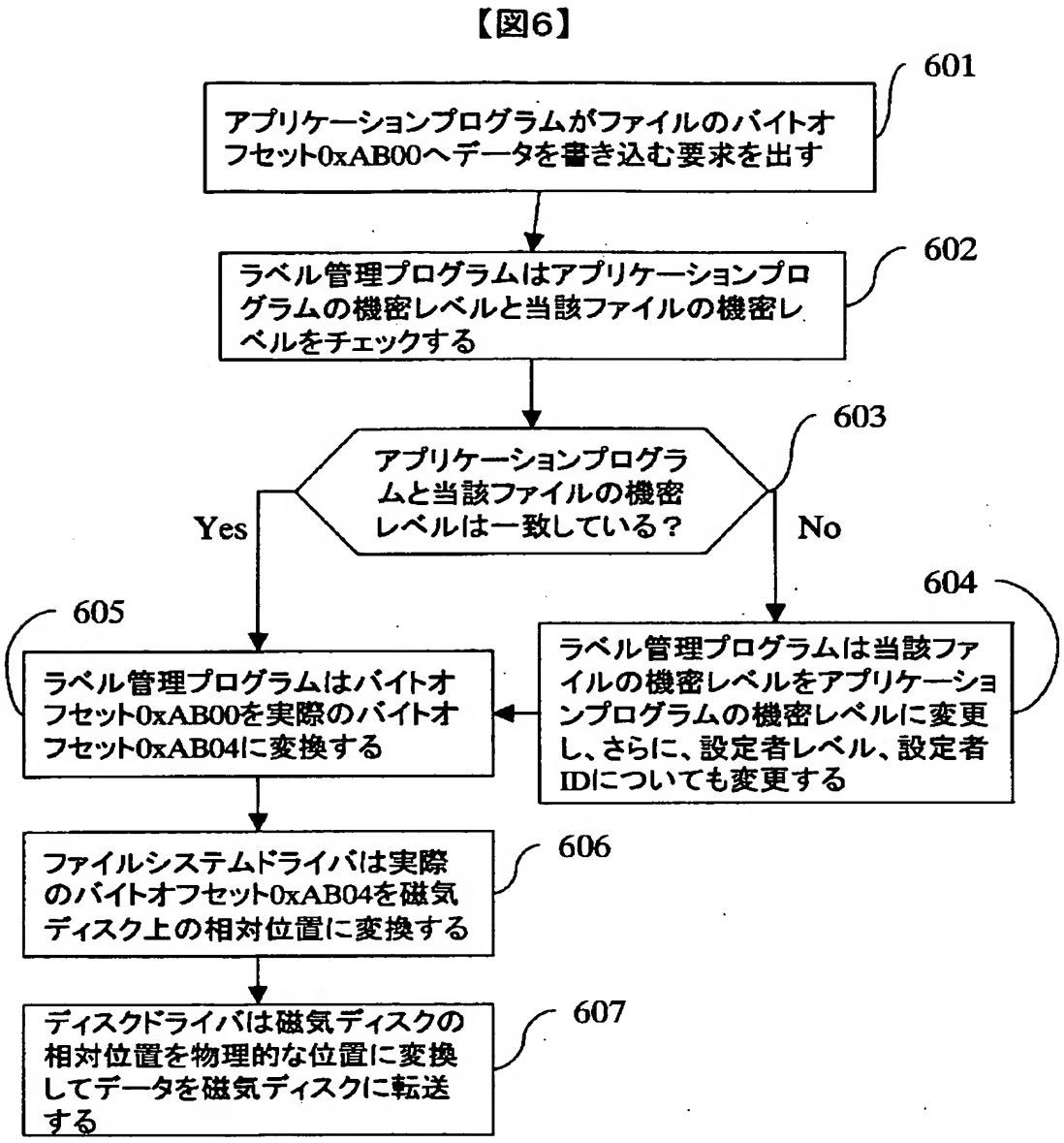
401 プロセスID	402 プロセス機密レベル	403 ファイル名	404 ファイルの機密レベル
FF053EC9	社外秘	C:¥document¥file1.dat	社外秘
		C:¥document¥file2.dat	一般
FF039D33	一般	C:¥document¥file3.dat	一般
・・・	・・・	・・・	・・・

【図５】

【図5】

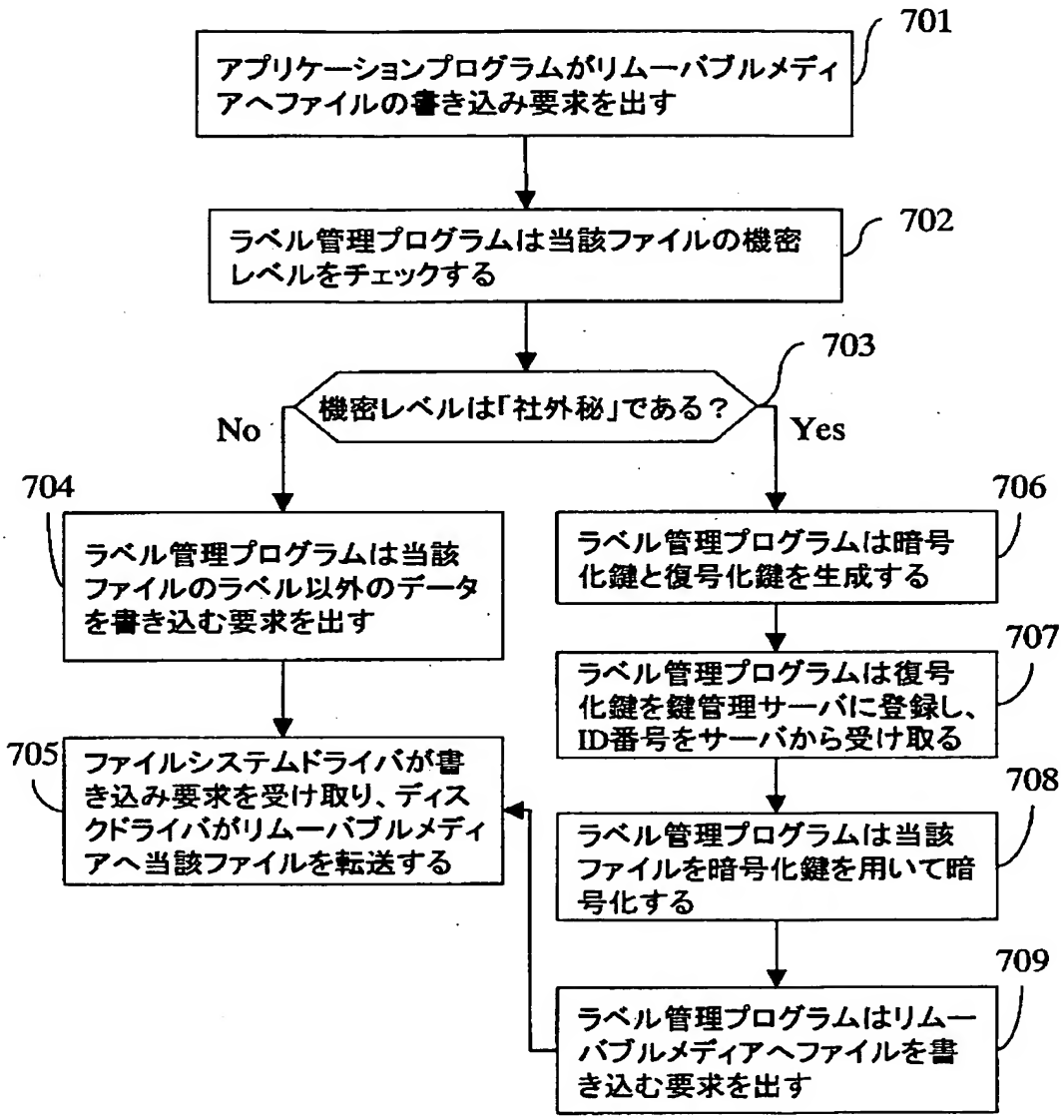


【図６】


【図6】
601
アプリケーションプログラムがファイルのバイトオフセット0xAB00へデータを書き込む要求を出す
602
ラベル管理プログラムはアプリケーションプログラムの機密レベルと当該ファイルの機密レベルをチェックする
603
アプリケーションプログラムと当該ファイルの機密レベルは一致している？
Yes
No
604
ラベル管理プログラムは当該ファイルの機密レベルをアプリケーションプログラムの機密レベルに変更し、さらに、設定者レベル、設定者IDについても変更する
605
ラベル管理プログラムはバイトオフセット0xAB00を実際のバイトオフセット0xAB04に変換する
606
ファイルシステムドライバは実際のバイトオフセット0xAB04を磁気ディスク上の相対位置に変換する
607
ディスクドライバは磁気ディスクの相対位置を物理的な位置に変換してデータを磁気ディスクに転送する

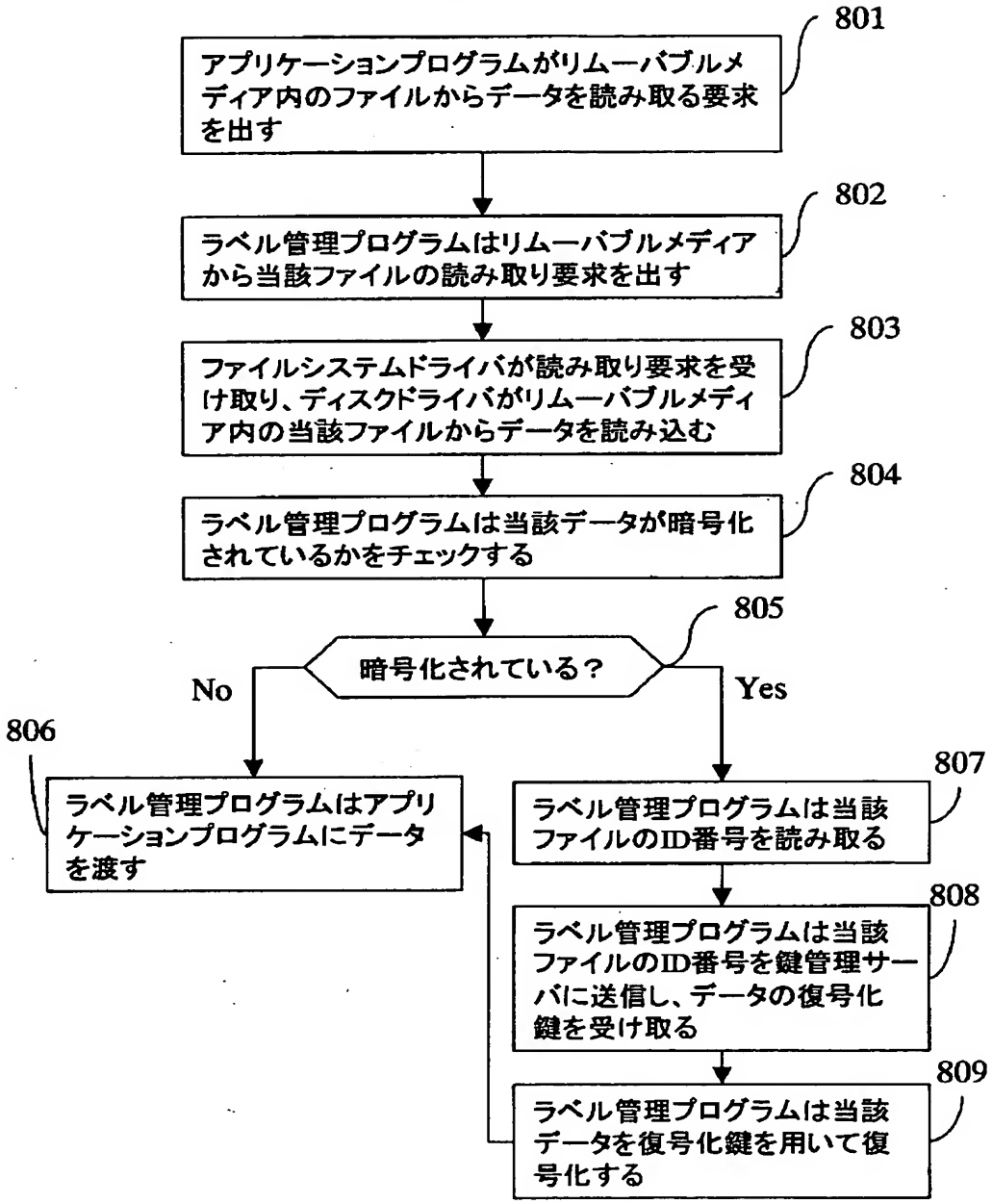
【図７】

【図7】


701
アプリケーションプログラムがリムーバブルメディアへファイルの書き込み要求を出す
702
ラベル管理プログラムは当該ファイルの機密レベルをチェックする
703
機密レベルは「社外秘」である？
No
Yes
704
ラベル管理プログラムは当該ファイルのラベル以外のデータを書き込む要求を出す
705
ファイルシステムドライバが書き込み要求を受け取り、ディスクドライバがリムーバブルメディアへ当該ファイルを転送する
706
ラベル管理プログラムは暗号化鍵と復号化鍵を生成する
707
ラベル管理プログラムは復号化鍵を鍵管理サーバに登録し、ID番号をサーバから受け取る
708
ラベル管理プログラムは当該ファイルを暗号化鍵を用いて暗号化する
709
ラベル管理プログラムはリムーバブルメディアへファイルを書き込む要求を出す

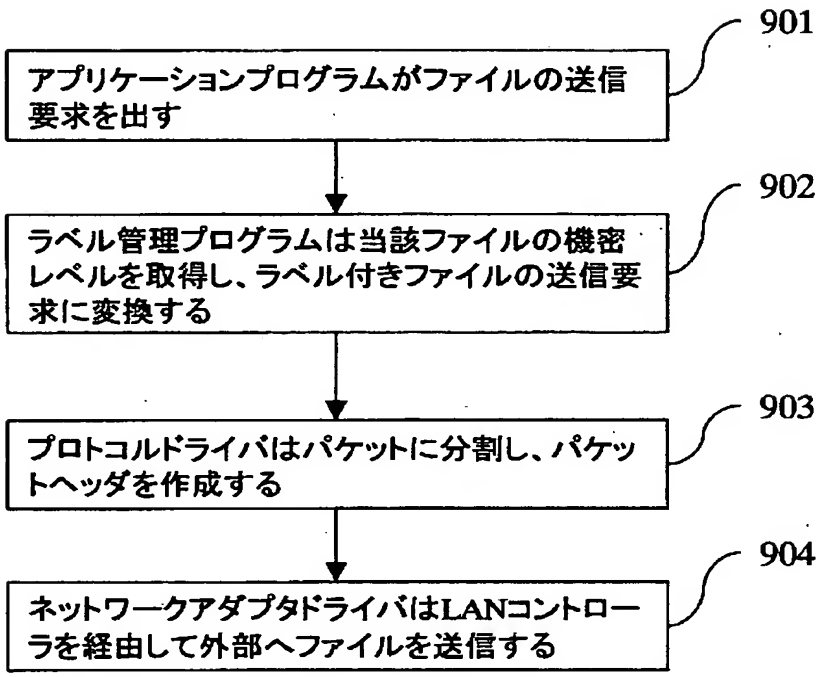
【図８】

【図8】


801
アプリケーションプログラムがリムーバブルメディア内のファイルからデータを読み取る要求を出す
802
ラベル管理プログラムはリムーバブルメディアから当該ファイルの読み取り要求を出す
803
ファイルシステムドライバが読み取り要求を受け取り、ディスクドライバがリムーバブルメディア内の当該ファイルからデータを読み込む
804
ラベル管理プログラムは当該データが暗号化されているかをチェックする
805
暗号化されている？
No
Yes
806
ラベル管理プログラムはアプリケーションプログラムにデータを渡す
807
ラベル管理プログラムは当該ファイルのID番号を読み取る
808
ラベル管理プログラムは当該ファイルのID番号を鍵管理サーバに送信し、データの復号化鍵を受け取る
809
ラベル管理プログラムは当該データを復号化鍵を用いて復号化する

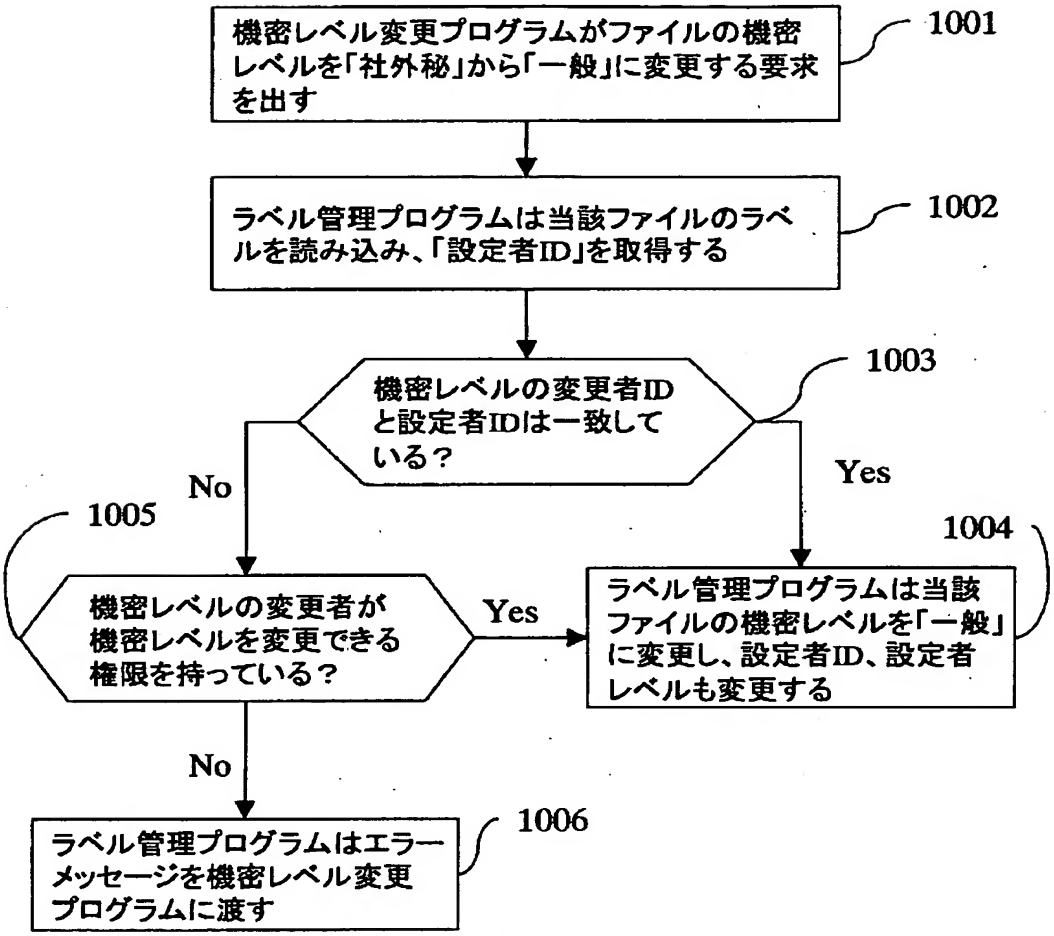
【図９】

【図9】


901
アプリケーションプログラムがファイルの送信要求を出す
902
ラベル管理プログラムは当該ファイルの機密レベルを取得し、ラベル付きファイルの送信要求に変換する
903
プロトコルドライバはパケットに分割し、パケットヘッダを作成する
904
ネットワークアダプタドライバはLANコントローラを経由して外部へファイルを送信する

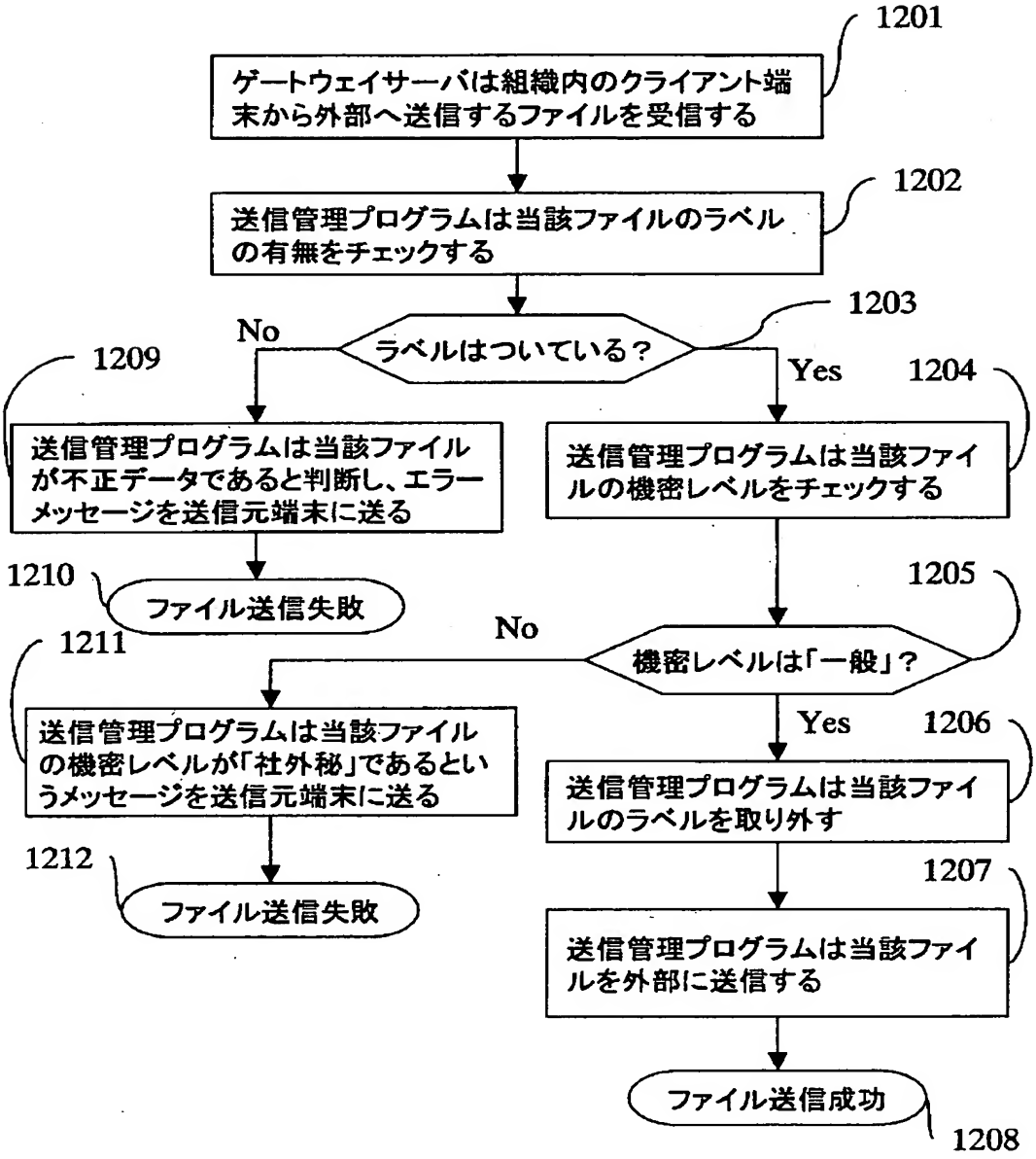
【図１０】

【図10】


機密レベル変更プログラムがファイルの機密レベルを「社外秘」から「一般」に変更する要求を出す
1001
ラベル管理プログラムは当該ファイルのラベルを読み込み、「設定者ID」を取得する
1002
機密レベルの変更者IDと設定者IDは一致している？
1003
Yes
No
1004
ラベル管理プログラムは当該ファイルの機密レベルを「一般」に変更し、設定者ID、設定者レベルも変更する
1005
機密レベルの変更者が機密レベルを変更できる権限を持っている？
Yes
No
ラベル管理プログラムはエラーメッセージを機密レベル変更プログラムに渡す
1006

【図１１】

【図11】


1201
ゲートウェイサーバは組織内のクライアント端末から外部へ送信するファイルを受信する
1202
送信管理プログラムは当該ファイルのラベルの有無をチェックする
1203
ラベルはついている？
No
Yes
1209
送信管理プログラムは当該ファイルが不正データであると判断し、エラーメッセージを送信元端末に送る
1204
送信管理プログラムは当該ファイルの機密レベルをチェックする
1210
ファイル送信失敗
1205
機密レベルは「一般」？
No
Yes
1211
送信管理プログラムは当該ファイルの機密レベルが「社外秘」であるというメッセージを送信元端末に送る
1206
送信管理プログラムは当該ファイルのラベルを取り外す
1212
ファイル送信失敗
1207
送信管理プログラムは当該ファイルを外部に送信する
ファイル送信成功
1208

【図１２】

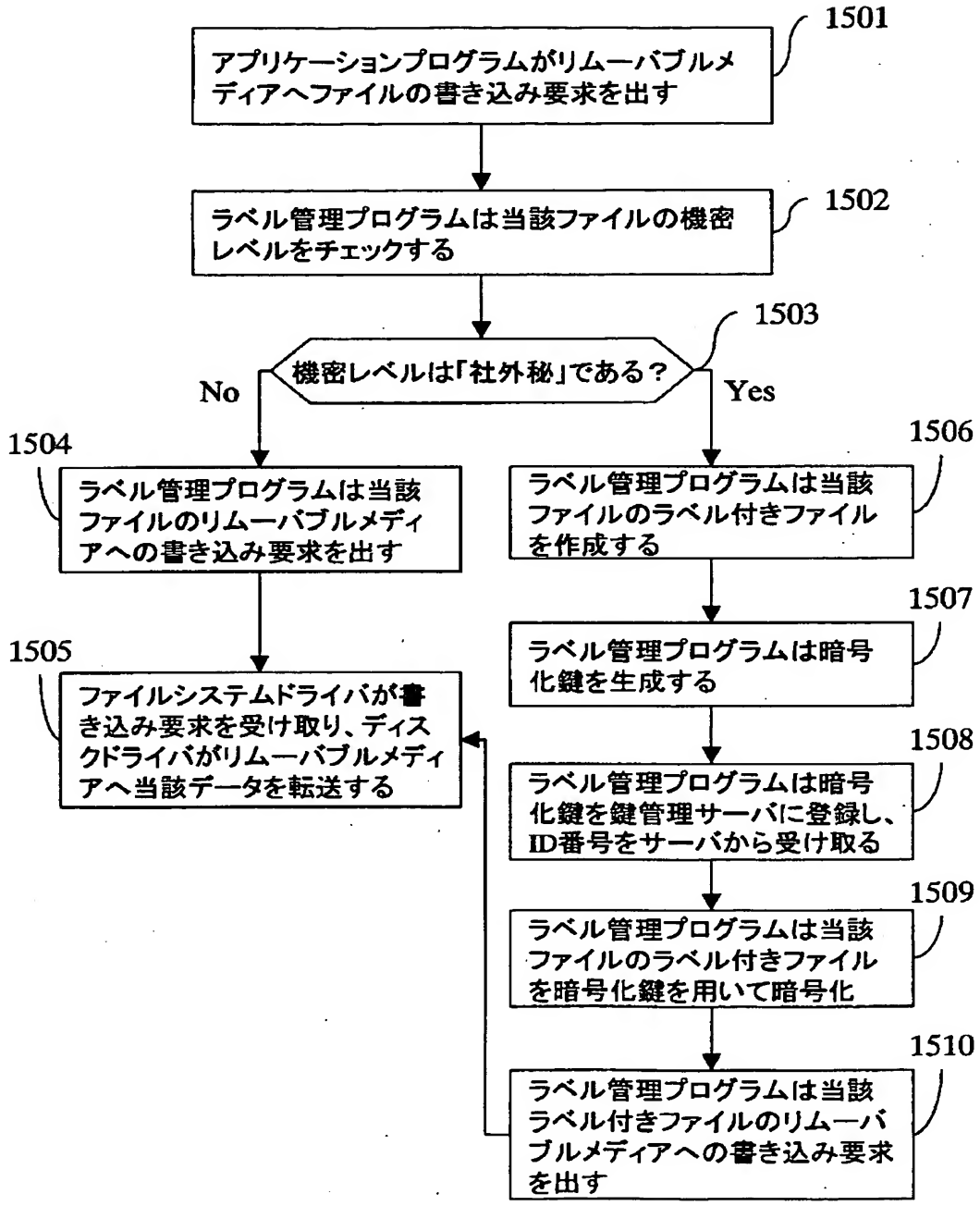
【図12】

1400

1401 ファイル名	1402 機密レベル	1403 設定者レベル	1404 設定者ID
C:¥document¥file1.dat	社外秘	一般	12345678
C:¥document¥file2.dat	一般	一般	12345678
・・・	・・・	・・・	・・・

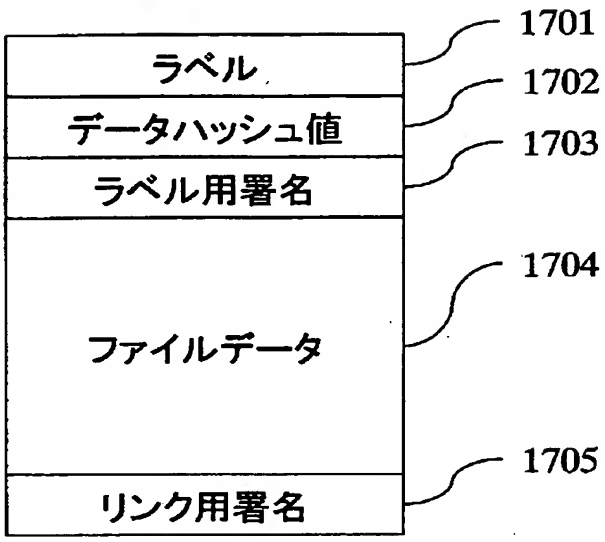
【図１３】

【図13】

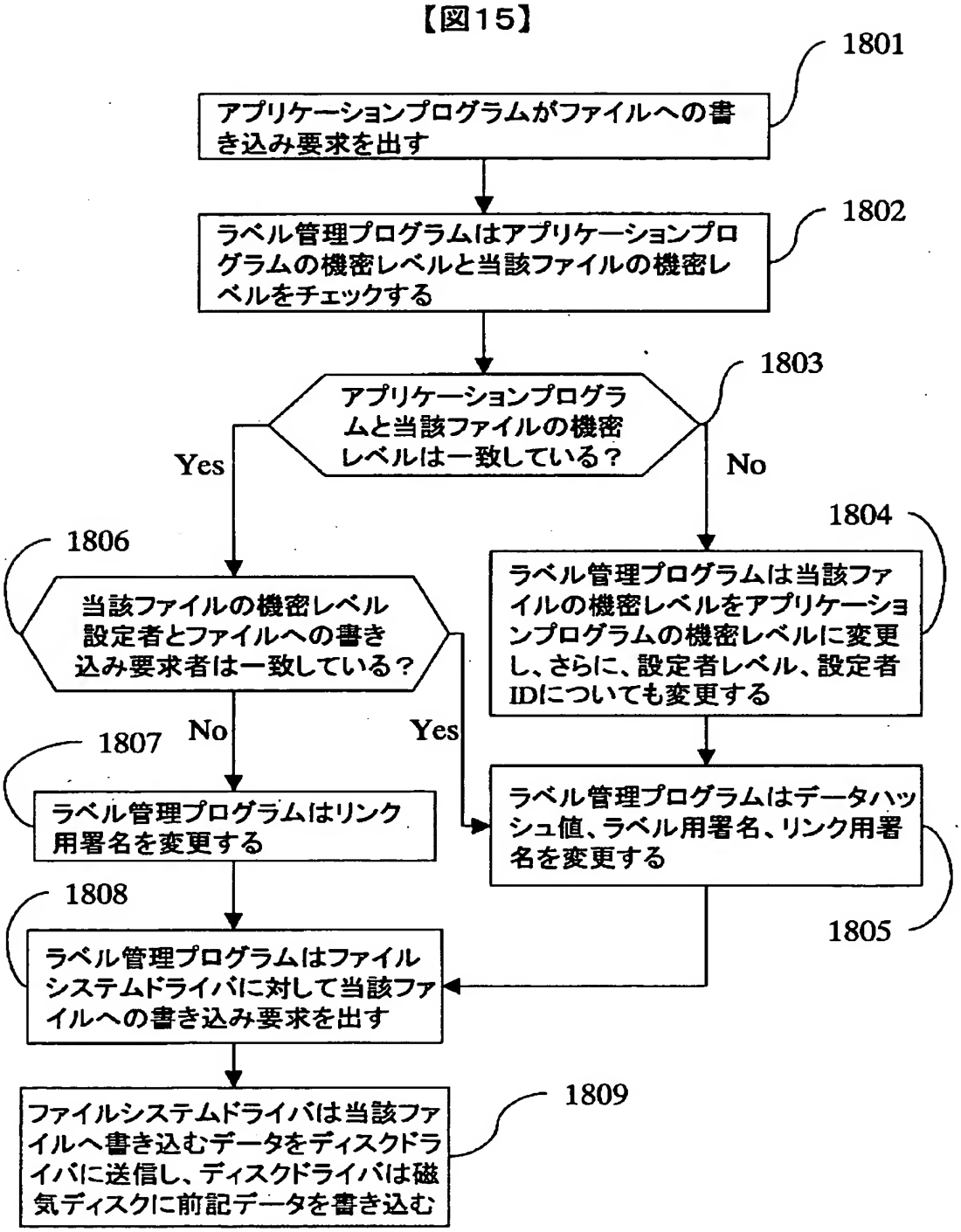

1501
アプリケーションプログラムがリムーバブルメディアへファイルの書き込み要求を出す
1502
ラベル管理プログラムは当該ファイルの機密レベルをチェックする
1503
機密レベルは「社外秘」である？
No
Yes
1504
ラベル管理プログラムは当該ファイルのリムーバブルメディアへの書き込み要求を出す
1505
ファイルシステムドライバが書き込み要求を受け取り、ディスクドライバがリムーバブルメディアへ当該データを転送する
1506
ラベル管理プログラムは当該ファイルのラベル付きファイルを作成する
1507
ラベル管理プログラムは暗号化鍵を生成する
1508
ラベル管理プログラムは暗号化鍵を鍵管理サーバに登録し、ID番号をサーバから受け取る
1509
ラベル管理プログラムは当該ファイルのラベル付きファイルを暗号化鍵を用いて暗号化
1510
ラベル管理プログラムは当該ラベル付きファイルのリムーバブルメディアへの書き込み要求を出す

【図１４】

【図14】

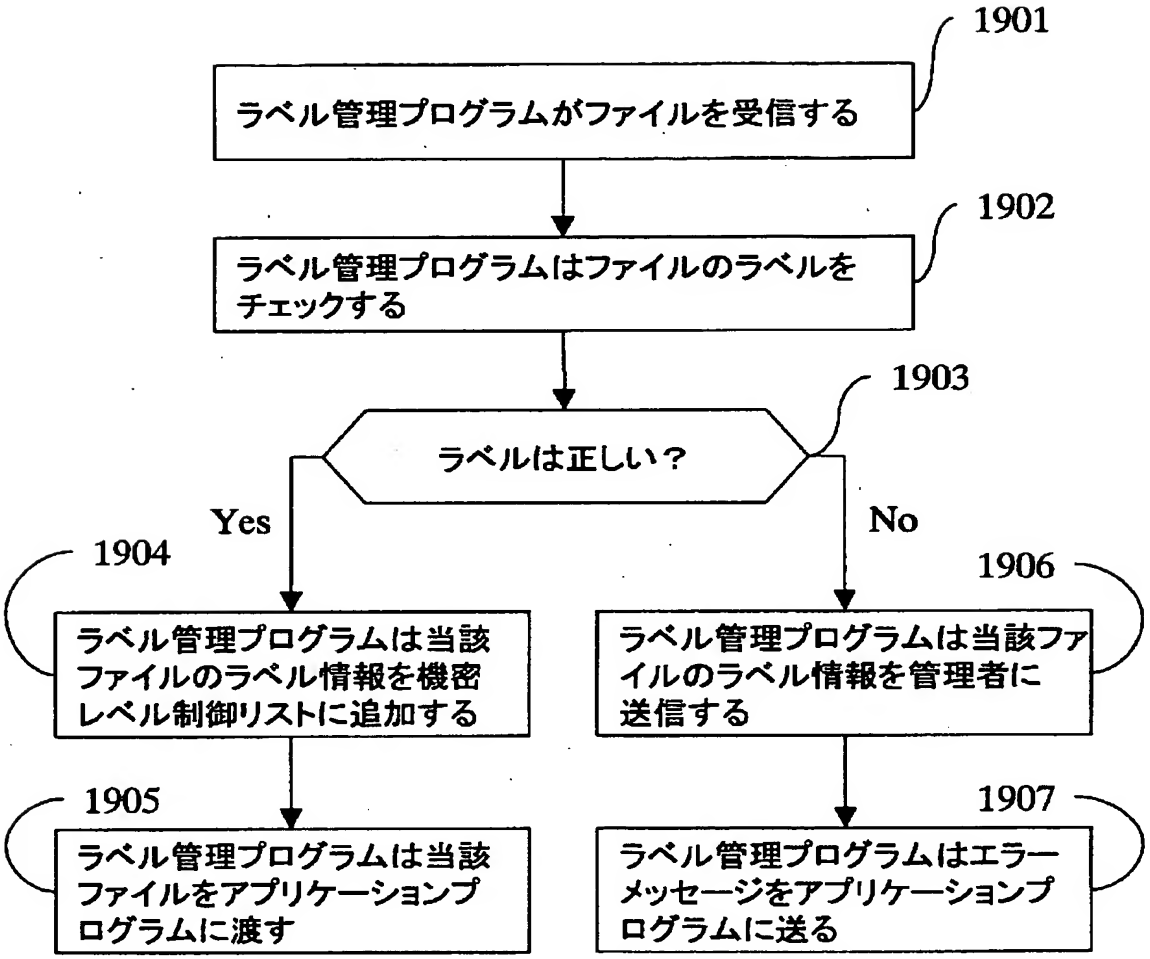

ラベル
データハッシュ値
ラベル用署名
ファイルデータ
リンク用署名
1701
1702
1703
1704
1705

【図１５】

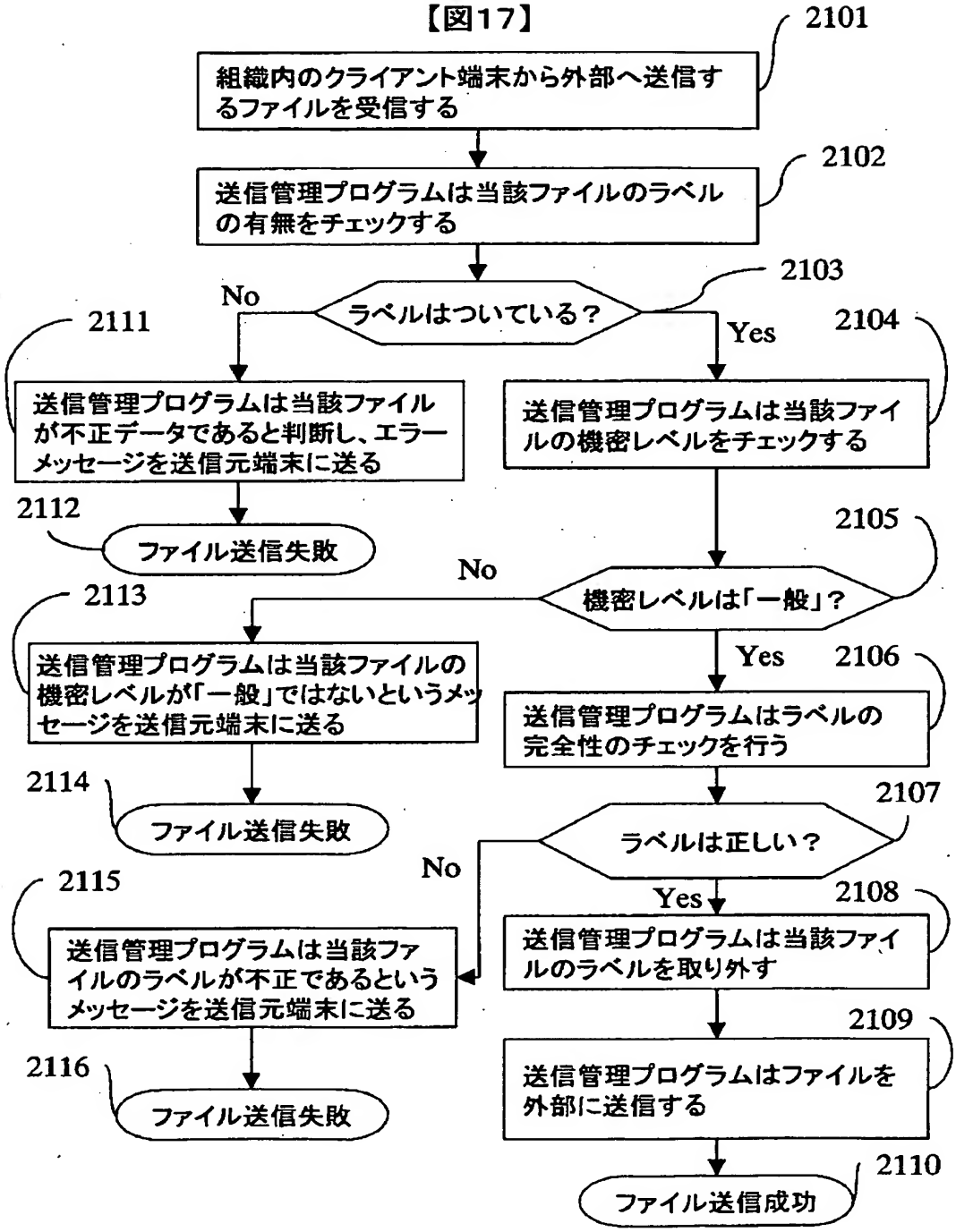

【図15】
1801
アプリケーションプログラムがファイルへの書き込み要求を出す
1802
ラベル管理プログラムはアプリケーションプログラムの機密レベルと当該ファイルの機密レベルをチェックする
1803
アプリケーションプログラムと当該ファイルの機密レベルは一致している？
Yes
No
1804
ラベル管理プログラムは当該ファイルの機密レベルをアプリケーションプログラムの機密レベルに変更し、さらに、設定者レベル、設定者IDについても変更する
1806
当該ファイルの機密レベル設定者とファイルへの書き込み要求者は一致している？
No
Yes
1807
ラベル管理プログラムはリンク用署名を変更する
ラベル管理プログラムはデータハッシュ値、ラベル用署名、リンク用署名を変更する
1805
1808
ラベル管理プログラムはファイルシステムドライバに対して当該ファイルへの書き込み要求を出す
ファイルシステムドライバは当該ファイルへ書き込むデータをディスクドライバに送信し、ディスクドライバは磁気ディスクに前記データを書き込む
1809

【図１６】

【図16】

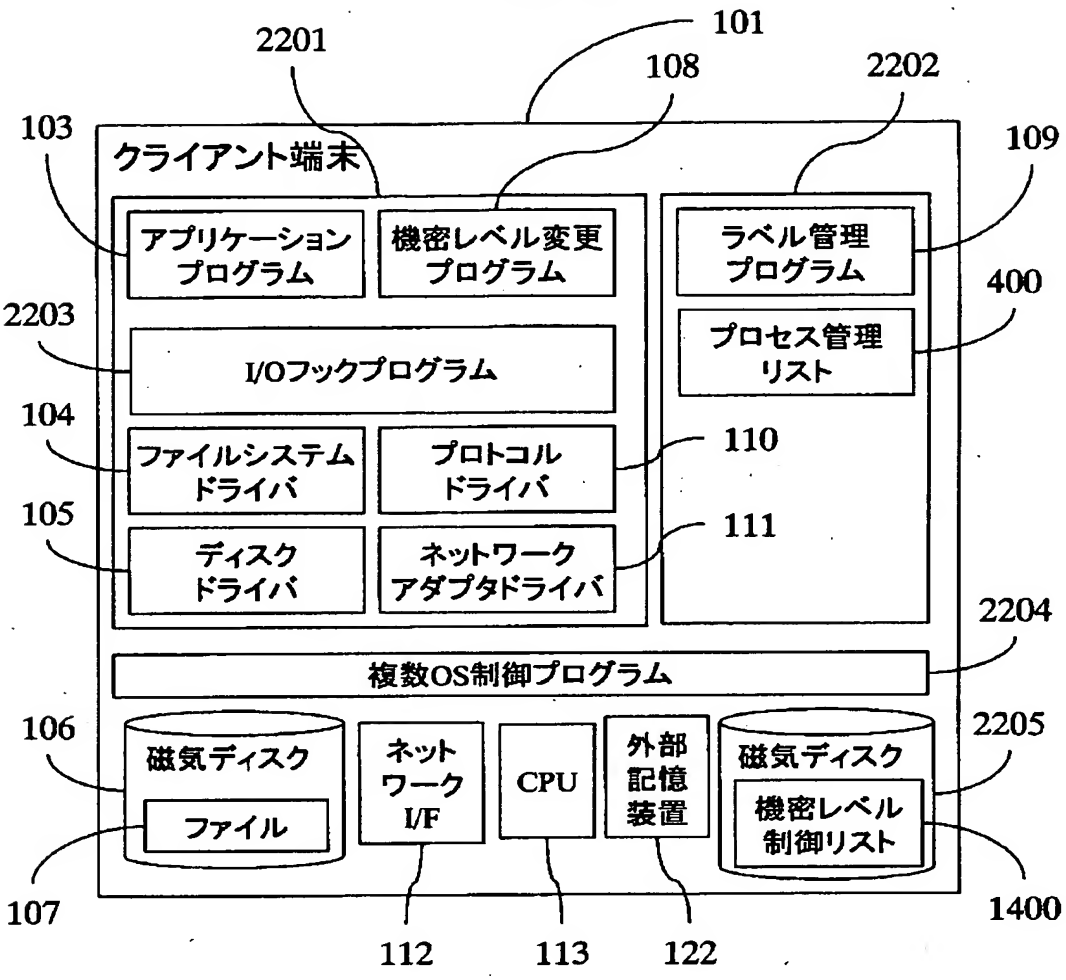

1901
ラベル管理プログラムがファイルを受信する
1902
ラベル管理プログラムはファイルのラベルをチェックする
1903
ラベルは正しい？
Yes
No
1904
ラベル管理プログラムは当該ファイルのラベル情報を機密レベル制御リストに追加する
1905
ラベル管理プログラムは当該ファイルをアプリケーションプログラムに渡す
1906
ラベル管理プログラムは当該ファイルのラベル情報を管理者に送信する
1907
ラベル管理プログラムはエラーメッセージをアプリケーションプログラムに送る

【図１７】


【図17】
2101
組織内のクライアント端末から外部へ送信するファイルを受信する
2102
送信管理プログラムは当該ファイルのラベルの有無をチェックする
2103
ラベルはついている？
No
Yes
2111
送信管理プログラムは当該ファイルが不正データであると判断し、エラーメッセージを送信元端末に送る
2104
送信管理プログラムは当該ファイルの機密レベルをチェックする
2112
ファイル送信失敗
2105
機密レベルは「一般」？
No
Yes
2113
送信管理プログラムは当該ファイルの機密レベルが「一般」ではないというメッセージを送信元端末に送る
2106
送信管理プログラムはラベルの完全性のチェックを行う
2114
ファイル送信失敗
2107
ラベルは正しい？
No
Yes
2115
送信管理プログラムは当該ファイルのラベルが不正であるというメッセージを送信元端末に送る
2108
送信管理プログラムは当該ファイルのラベルを取り外す
2109
送信管理プログラムはファイルを外部に送信する
2116
ファイル送信失敗
2110
ファイル送信成功

【図１８】

【図18】


2201
101
108
2202
103
クライアント端末
109
アプリケーション
プログラム
機密レベル変更
プログラム
ラベル管理
プログラム
400
2203
I/Oフックプログラム
プロセス管理
リスト
104
ファイルシステム
ドライバ
プロトコル
ドライバ
110
105
ディスク
ドライバ
ネットワーク
アダプタドライバ
111
2204
複数OS制御プログラム
106
磁気ディスク
ファイル
ネット
ワーク
I/F
CPU
外部
記憶
装置
磁気ディスク
機密レベル
制御リスト
2205
107
112
113
122
1400

【書類名】要約書

【要約】

【課題】

送信者の不注意による機密ファイルの漏洩を防止すると同時に、任意のファイルフォーマットに対して対応可能なネットワークシステムを提供する。

【解決手段】

クライアント端末１０１内のファイル１０７に機密レベル（機密、非機密）を表すラベルを付け、クライアント端末１０１はラベル付きファイル１０７を外部へ送信する。ゲートウェイサーバ１１８上の送信管理プログラム１１９がファイル１０７のラベルのチェックを行い、機密レベルが非機密の場合に組織外ネットワーク１２１へファイル１０７を送信する。また、ラベル管理プログラム１０９がクライアント端末１０１内のラベル付きファイル１０７の管理を行う。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００１－３７０８２４
受付番号	５０１０１７８２６６４
書類名	特許願
担当官	第八担当上席　００９７
作成日	平成１３年１２月　６日

＜認定情報・付加情報＞

【提出日】　平成13年12月 5日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所